WASH—1400
(NUREG-75/014)

Reactor Safety Study

An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants

Appendices III and IV

United States Nuclear Regulatory Commission

October 1975

Available from
National Technical Information Service
Springfield, Virginia 22161
Price: Printed Copy $6 00 . Microfiche $2 25

Second printing

WASH–1400
(NUREG-75/014)

FAILURE DATA

APPENDIX III

to

REACTOR SAFETY STUDY

U.S. NUCLEAR REGULATORY COMMISSION

OCTOBER 1975

Appendix III

Table of Contents

Section		Page No.
1.	FAILURE DATA	III-1
	1.1 Discussion of Contents	III-1
	1.2 Definition and Explanation of Terms	III-1
	1.3 General Data Considerations	III-2
2.	DATA BASE ASSESSMENTS	III-5
	2.1 Overall Data Tabulation	III-5
	2.2 Data Assessment Comparison	III-5
3.	CURRENT NUCLEAR EXPERIENCE	III-15
	3.1 Introduction	III-15
	3.2 Nuclear Experience Statistics	III-15
	3.3 Operating Incidents Used for Statistical Analyses and Individual Failure Analysis	III-19
	3.4 Individual Failure Analysis Listing	III-25
REFERENCES		III-33
4.	EXPANDED FINAL DATA ASSESSMENT	III-39
	4.1 Introduction	III-39
	4.1.1 Notes on Pumps	III-39
	4.1.2 Notes on Valves	III-40
	4.1.3 Notes on Pipe - Testing	III-41
	4.1.4 Notes on Motors	III-41
	4.1.5 Notes on Relays - Failure Modes	III-41
	4.1.6 Notes on Switches - Failure Modes	III-41
	4.1.7 Notes on Batteries - Failure Modes	III-41
	4.1.8 Notes on Solid State Devices	III-41
	4.1.9 Notes on Diesels	III-42
	4.1.10 Notes on Instrumentation - Failure Modes	III-42
	4.1.11 Notes on Wires and Terminal Boards - Failure Modes	III-42
	4.2 Summary of Post Accident Assessments	III-42
	4.2.1 Notes on Containment Hardware - Test	III-42
	4.2.2 General Data Behavior	III-42
REFERENCES		III-43
5.	TEST AND MAINTENANCE DATA AND APPLICATIONS	III-53
	5.1 Introduction	III-53
	5.2 Corroboration of the Model Results	III-54
6.	SPECIAL TOPICS	III-59
	6.1 Human Reliability Analysis	III-59
	6.1.1 Introduction	III-59
	6.1.2 Human Performance Data	III-59
	6.1.3 Performance-Shaping Factors	III-62

Table of Contents (Continued)

Section			Page No.
		6.1.3.1 Level of Presumed Psychological Stress	III-63
		6.1.3.2 Quality of Human Engineering of Controls and Displays	III-63
		6.1.3.3 Quality of Training and Practice	III-64
		6.1.3.4 Presence and Quality of Written Instructions and Method of Use	III-64
		6.1.3.5 Coupling of Human Actions	III-65
		6.1.3.6 Type of Display Feedback	III-66
		6.1.3.7 Personnel Redundancy	III-66
	6.1.4	A Sample Hunan Reliability Analysis	III-67
6.2		Aircraft Crash Probabilities	III-69
	6.2.1	Number and Nature of Aircraft Movements	III-70
	6.2.2	Determination of Plant Vulnerable Area	III-70
	6.2.3	Damage Potential	III-70
	6.2.4	Typical Damage Calculation (Surry 3 and 4)	III-70
		6.2.4.1 Source	III-70
		6.2.4.2 Source	III-70
6.3		Total Loss of Electric Power	III-71
	6.3.1	Total Loss of Electric Power at LOCA	III-71
	6.3.2	Total Loss of Electric Power During a LOCA	III-72
	6.3.3	Summary	III-73
6.4		Pipe Failure Data	III-74
	6.4.1	Plant Parameters	III-75
	6.4.2	Nuclear and Nuclear-Related Experience	III-75
	6.4.3	U.S. Non-Nuclear Utility Experience	III-76
	6.4.4	United Kingdom Data	III-77
	6.4.5	Other Reported Pipe Failure Rates	III-78
6.5		Failure Rates Compared With Log Normal	III-78
REFERENCES			III-78
7.		REFERENCES	III-91
7.1		Discussion of References	III-91
7.2		General Sources	III-91
7.3		Special Sources	III-91

List of Tables

Table		Page No.
III 2-1	Data Assessment Tabulation	III-7/8
III 2-2	Comparison of Assessments with Nuclear Experience	III-11/12
III 2-3	Comparison of Assessments with Industrial Experience	III-13/14
III 3-1	Number of Failures by Plant Showing Failures During Standby and Operations	III-35/36
III 3-2	Number of Failures by Plant Component/System	III-35/36
III 3-3	Averaged Failure Rate Estimates (Rounded to Nearest Half Exponent)	III-35/36
III 3-4	Averaged Demand Probability Estimates (Rounded to Nearest Half Exponent)	III-35/36
III 3-5	1972 Failure Categorization Into Random Versus Common Mode	III-37/38
III 3-6	Common Mode Effects and Causes	III-37/38
III 4-1	Summary of Assessments for Mechanical Hardware	III-45/46
III 4-2	Summary of Assessments for Electrical Equipment	III-47/48
III 4-3	Summary of Post Accident Assessments	III-49/50
III 5-1	Summary of Test Act Duration	III-55/56
III 5-2	Summary of Major Maintenance Act Duration (Raw Data)	III-55/56
III 5-3	Log-Normal Modeled Maintenance Act Duration	III-55/56
III 6-1	General Error Rate Estimates	III-81/82
III 6-2	Aircraft Crash Probabilities	III-81/82
III 6-3	Comparison of Probability of an Aircraft Crash for Various Types of Aircraft	III-81/82
III 6-4	Crash Probabilities at Various Sites	III-81/82
III 6-5	Summary of Transmission Line Outages (Based on Bonneville Power Administration Data--1970 Statistics)	III-83/84
III 6-6	Summary of Transmission Line Outages (Based on Bonneville Power Administration Data--1971 Statistics)	III-83/84
III 6-7	Summary of Transmission Line Outages (Based on Bonneville Power Administration Data--1972 Statistics)	III-83/84
III 6-8	Probability of Total Loss of Electric Power After A LOCA	III-83/84
III 6-9	Pipe Failure Assessed Values	III-83/84
III 6-10	Reported Pipe Failure Rates	III-85/86

List of Figures

Figure		Page No.
III 4-1	Relative Failure Rate Assessments - Switches.....	III-51/52
III 4-2	Relative Failure Rate Assessments - Valves.....	III-51/52
III 4-3	Relative Failure Rate Assessments - Pumps.....	III-51/52
III 4-4	Demand Probabilities of Classes of Hardware.....	III-51/52
III 4-5	Leak and Rupture Assessments for Passive Hardware.....	III-51/52
III 5-1	Observed Repair Times and Theoretical Distribution - Pumps.....	III-57/58
III 5-2	Observed Repair Times and Theoretical Distribution - Valves.....	III-57/58
III 5-3	Observed Repair Times and Theoretical Distribution - Diesels.....	III-57/58
III 5-4	Observed Repair Times and Theoretical Distribution - Instrumentation.....	III-57/58
III 6-1	Hypothetical Relationship Between Performance and Stress.....	III-87/88
III 6-2	Motor Operated Valve (MOV) Switches on Control Panel.....	III-87/88
III 6-3	Probability Tree Diagram for Step 4.8.1.....	III-87/88
III 6-4	Cumulative Outage Duration Distribution Curve.....	III-87/88
III 6-5	Histogram - Restoration of Transmission Line Outages.....	III-87/88
III 6-6	Log-Normal Distribution - Pumps.....	III-89/90
III 6-7	Log-Normal Distribution - Valves.....	III-89/90
III 6-8	Log-Normal Distribution - Clutch - Electrical.....	III-89/90
III 6-9	Log-Normal Distribution - Diesels.....	III-89/90

Section 1

Failure Data

In the quantitative system probability estimates performed in this study, component behavior data in the form of failure rates and repair times are required as inputs to the system models. Since the goal of this study is risk assessment, as opposed to reliability analysis, larger errors (e.g. order of magnitude type accuracy) can be tolerated in the quantified results. This has important implications on the treatment of available data. In standard reliability analysis, point values (i.e., "best-estimates") are generally used for both data and results in quantifying the system model.

In risk assessment, since results accurate to about an order of magnitude are sufficient, data and results using random variable and probabilistic approaches, can be usefully employed. The base of applicable failure rate data is thus significantly broadened since data with large error spreads and uncertainties can now be utilized. The data and associated material that were assembled for use in this study and that are presented here are to be used in the random variable framework (which will be described). The data and the accompanying framework are deemed sufficient for the study's needs. Care must be taken, however, since this data may not be sufficiently detailed, or accurate enough for use in general quantitative reliability models.

1.1 DISCUSSION OF CONTENTS

The items listed below summarize the detail sections which follow.

1. A listing of definitions and a discussion of the general treatment of data within the random variable approach as utilized by the study. (section 1)
2. A tabulation of the assessed data base containing failure classifications, final assessed ranges utilized in quantification and reference source values considered in determining the ranges. Additional tables, extracted from the main table, are also given showing the assessed ranges and comparing them with industrial and nuclear experience. (section 2)
3. A discussion of nuclear power plant experience that was used to validate the data assessment by testing its applicability as well as to check on the adequacy of the model to incorporate typical real incidents. (section 3)
4. An expanded presentation of the data assessment giving information on applicability considerations. Detailed characteristics are also given for utilization of the data in the random variable approach. Graphs are finally presented showing trends and class behaviors. (section 4)
5. A discussion of test and maintenance data including comparisons of models with experience data. (section 5)
6. Special topics, including assessments required for the initiating event probabilities and human error data and modeling. (section 6)

1.2 DEFINITION AND EXPLANATION OF TERMS

Listed below are definitions of terms which will be employed in the discussions. Certain of these definitions are listed elsewhere, but have been restated here since they have pertinence with regard to data assessment.

Failure Probability: the probability that a system, subsystem, or component will suffer a defined failure in a specified period of time. In context of the defined failure, the failure probability is equivalent to the unreliability.

Unavailability: the probability that a system, subsystem, or component will not be capable of operating at a particular time, i.e., will be in a failed state. Availability is the complement of unavailability. Point unavailability and interval unavailability are treated as being equivalent here (see the fault tree quantification discussion for further details).

Active Devices: those operating devices such as pumps, valves, relays, etc.,

that run, transfer, or change state to perform their intended function.

Passive Devices: those inert devices such as pipes, vessels, welds, etc., that are generally inactive but whose failure will affect system behavior.

Test Time: the total on-line time required to test a system, subsystem, or component. This total includes the active test time plus the on-line time required to reconfigure before and after testing.

Maintenance Time: the total on-line time required to maintain a system subsystem, or device. Analogous to the previous test definition, the on-line maintenance period includes actual maintenance time plus any adjustment or check-out time associated with the maintenance.[1]

Test Interval: the length of time between tests of systems, subsystems, and components. For the applications here, this interval is often 720 hours, (∿1 month), although there are exceptions, and relevant test intervals must be obtained for each component. As will be further discussed, test intervals are treated as being periodic.

Maintenance Interval: the length of time between maintenance on systems, subsystems, or components. The interval depends upon whether the maintenance is of periodic, non-periodic, scheduled or non-scheduled nature. For the applications here, the maintenance interval is generally treated as being non-scheduled and hence non-periodic.

Demand Probabilities: the probability that the device will fail to operate upon demand for those components that are required to start, change state, or function at the time of the accident. The demand probabilities, denoted by Q_d, incorporate contributions from failure at demand, failure before demand, as well as failure to continue operation for a sufficient period of time for successful response to the need. When pertinent, the demand data Q_d can be associated with standard cyclic data or can be interpreted as a general unavailability. Human error data can also be associated with demand probabilities (i.e. per action) as discussed in the human evaluation section.

Operating Failure Rates: for those components required to operate or function for a period of time, the probability (per hour) of failure is denoted by λ_o. For those components affected by accident environments, additional failure rates applicable to the pertinent accident environment are given.

Standby Failure Rates: for those passive-type devices such as pipes, wires, etc., which are normally dormant or in standby until tested or an accident occurs, the probability (per hour) of failure is denoted by λ_s.

The above definitions involve the standard terminologies and concepts employed in reliability theory. Test and maintenance data in general consists of the test and maintenance times and the test and maintenance intervals. Component failure data in general consists of the demand probabilities, operating failure rates, and standby failure rates. The characteristics which have been described are by no means exhaustive. Also, many equivalent bases can be constructed. The characteristics as defined here, however, are sufficient for the applications in the study.

1.3 GENERAL DATA CONSIDERATIONS

This section describes certain basic concepts involving the probabilistic, or random variable approach used in the study and its implications with regard to the establishment of a data base.

The quantitative evaluation of a system can involve one of two types of calculations: a point calculation, or a random variable evaluation. The point and random variable types of evaluation differ with regard to basic goals and approaches and how to input data must be prepared. With point value calculations the general goal is to derive a best value for the system parameter of interest, usually the system unavailability or failure probability (unreliability). In point calculations one attempts to obtain the input data with great accuracy since, the computed results are to represent an exact type of value. In reality, of course, point values are never exact but are computed as precisely as possible.

---

[1] The term "on-line", as standardly used, denotes the time actually impacting the system unavailability or failure probability. The "on-line" phrase is often deleted with the understanding that only test or maintenance time actually affecting the system is included.

Because of the need for highly accurate component assessment, point calculations generally require extensive input data which classify each component according to particular characteristics, known as the "pedigree" of the component. Examples of these characteristics are:

a. Generic type of component (relay, motor, etc.)

b. Component manufacturer

c. Component failure mode (i.e., opens, closes, ruptures, etc.)

d. Component specifications (i.e., voltage, flow rate, etc.)

e. Component environment (i.e., temperature, humidity, etc.)

In point calculations, a single value for each component failure rate or demand probability is obtained. Once obtained, these values are then substituted into the reliability equations to then obtain the point value for the system result. In practice, to obtain a single failure rate or demand probability value for a particular component, new failure data is collected in the form of samples, and statistical point estimation techniques are used.[1]

In practice, an exact match of the pedigree characteristics is not always possible, and a failure rate is derived from data which matches, as closely as possible, the important characteristics of the problem. Engineering judgment is used to determine the applicability of the various data. The source data used in point evaluations may be obtained from handbooks, field experience, or from specially designed sampling experiments.

The second approach, the random variable technique, is not commonly discussed and treated in reliability texts but is a standard general technique in statistical and probabilistic modeling. In the random variable approach, one point value for an input data parameter is seen as being insufficient to describe the applicable situation. Instead a range of values is determined which describes the variability and randomness associated with the parameter. The data parameter which is input to a calculation, such as a failure rate, is thus now treated as being a random variable and the range of values gives the various possibilities for the random variable. As a last step, probability distribution is associated with the random variable to describe the probability associated with various possible values.

One of the simplest ways to obtain necessary data for the random variable approach is to estimate ranges for each piece of data which is to be used. In reliability applications of the random variable approach, failure data is treated as being a random variable and hence estimation involves obtaining ranges for each component failure rate and each demand probability.

The random variable approach was chosen in the study for several reasons. The reliability results which were computed were to apply to a population of reactor plants (100) and hence it was desired to model the component failure variability from plant to plant. Also, data which does exist is not precise but shows large uncertainty and variability and it was desired to incorporate this uncertainty and variability.

Treating data as random variables is sometimes associated with the Bayesian approach where the data distributions are treated as priors. The system failure probability and its unavailability are subsequently treated as conditional probabilities and the overall marginal distribution is obtained by integration over the data priors. Because the data distributions were associated with a population (the 100 reactor plants) the data and system characteristics were treated by the study as being simply random variables, however the Bayesian interpretation can also be used where the data distributions are treated as given Bayesian priors.

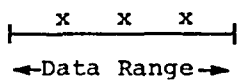
The failure rates and demand probabilities used in the study were derived from handbooks, reports, operating experience, and nuclear power plant experience. The data sources involved Department of Defense data (Navy, Air Force, etc.), NASA data and general industrial operating experience as well as nuclear power plant data. The assessment process entailed an amalgamation of this information to obtain final ranges which described regions in which the data had a high probability of lying.

Examination of the various sources of component data showed that, in assess-

---

[1] Standard approaches involve parametric estimation techniques, such as maximum likelihood.

ment of the final data base, only order of magnitude accuracy would be generally feasible. However, these accuracies were sufficient for the risk calculations since only order of magnitude results are required. In arriving at the final data assessment, the fact that ranges were assigned to each data variable gave latitude for the incorporation of differing data source values. A heuristic illustration is shown below of the range type of assessment. The range type of assessment has the advantage of rendering the calculations and results to be insensitive to fine distinctions of the applicability of any particular bit of data.



As discussed in Appendix II, the log normal distribution was used to describe the data variability. Since the log normal has two parameters (the mean and standard deviation, say), the two end points of a suitably defined range determine the unique, applicable log normal. A 90% range was selected for the assessments with the lower range end point being the 5% bound and the upper end point the 95% bound. The range which was assessed for each failure rate and demand probability thus coincided with this 90% definition (there was thus a 90% probability that the data value would be in this range).

Even though the data sources used, represented diverse conditions and applications, with some sources apparently more applicable than others, the data sources were in general agreement within one to two orders of magnitude accuracy. The final assessed ranges were thus generally one to two orders of magnitude in width to represent this degree of data consistency. Because of the order of magnitude accuracies, range end points were determined to the nearest half integer on the exponent scale, i.e. a failure rate end point being 10^{-1} or $10^{-1.5}$, etc. This half integer exponent scale coincided with the assignment of a 3 or 1 for the significant number, i.e. 1×10^{-1} or 3×10^{-2}, etc.

Since diverse data sources were used and since a large number of components were involved in the assessment, a number of iterations were involved in obtaining the actual assessed ranges. In assessing the ranges, data points were selected from the various sources, including nuclear experience, and a range was then overlayed to cover approximately 90% of the points. As described in Appendix II, the calculations are not sensitive to the precise 90% definition, for example little differences were obtained if the range was actually 85% or 95%. The range determinations involved data plotting with decisions made on the weight of each source data point. The assessment decisions were based upon the experience of individuals involved in reliability and nuclear power plant operation.

Because of the order of magnitude ranges and accuracies, components were generally classified only to generic type. When extreme behaviors existed, component failure definitions were further detailed. When available, actual nuclear plant experience was used as the principal basis in determining and checking the final assessed ranges. Nuclear component variability from plant to plant that was observable was not inconsistent with the final range widths. (This variability was also not inconsistent with the random variable approach utilized.)

The tables and discussions which follow, present the basic data, assessed ranges, and comparisons involving the assessed ranges. This hopefully will aid the reader in determining for himself the validity of the data ranges that were employed.

In the tables and discussions, the extractable failure modes are given for each component classification. Failure rates are in units of per hour HR^{-1} and demand probabilities (unavailabilities) are in units of per demand D^{-1}. The lower and upper bounds which are given coincide with the approximate 5% and 95% range end points (to half integer scale). The ranges and upper and lower bounds can be interpreted as a confidence on the data, however, this must be done so within the random variable (or Bayesian) framework in which the data is to be applied.

Section 2

Data Base Assessments

2.1 OVERALL DATA TABULATION

Table III 2-1 shows the final assessed ranges employed by the study and the principal, raw input values that formed the bases for the assessed ranges.

2.2 DATA ASSESSMENT COMPARISON

Tables III 2-2 and III 2-3 contain extractions from Table III 2-1 and show more explicitly the final assessed ranges as compared to obtainable nuclear experience values and extreme values from industrial experience. The nuclear values were computed from current nuclear experience as discussed in the subsequent section. The industrial bounds represent the extreme minimum and maximum values obtained from the raw industrial source inputs (which are deterministic type bounds) and are compared with the assessed ranges (which are defined at 90% probability).

TABLE III 2-1 Data Assessment Tabulation

FAILURE MODES		ASSESSMENT MEDIAN	LOWER UPPER BOUND	UK NUC OPERATING EXPERIENCE 1, 2, 3	AVCO 6	FARADA 5	LMEC 7	SRI 4	COLLINS NUC 8	HOLMES HAYNES 9	PIONEER 20	CHEM ENGR UK-CHEM 10, 11	SHOPS UK-NUC 34	BOURNE UK 35	UNDERAKES GERMANY 36	DAVIL 37	EUROPE NUC AGENCY 38	PUGH 39	STERAP UK-CHEM 40	MOORE 41	IEEE TRANS UK-NUC 42a	IEEE TRANS GER 42b	BOURNE UK 43	DYNAY 44	FARMER UK GAS 45	BEATTIE 46	BEH 47	SPEIT IV 48	HEADINGTON 49	GULF 50	PROCEEDING 51		NRTS IDAHO 52
	Pumps — Failure To Start	1×10^{-3}/D	3×10^{-4} 3×10^{-3}	1×10^{-3}/D	5×10^{-3}	1×10^{-3}	3×10^{-3}	3×10^{-3}		1×10^{-4}	NA		5×10^{-6}	6×10^{-4}	4×10^{-3}	1×10^{-3}	4×10^{-4}	1×10^{-3}	NA	NA	NA	NA	NA	2×10^{-4}	NA	NA	NA	NA	NA	NA		
	Pumps — Failure To Run — Normal	3×10^{-6}/HR	3×10^{-6} 3×10^{-4}	3×10^{-6}/HR	1.3×10^{-5}	3×10^{-6}	1.4×10^{-4}	1×10^{-5}		3×10^{-6}	NA		1.4×10^{-7}	2×10^{-6}	1×10^{-5}	3×10^{-6}	1×10^{-6}	3×10^{-6}	NA	NA	NA	NA	NA	6×10^{-6}	NA	NA	NA	NA	NA	NA	4×10^{-6}		
	Pumps — Failure To Run — Extreme ENV	1×10^{-3}/HR	1×10^{-4} 1×10^{-2}			3×10^{-4}	1×10^{-3}				NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-4}
	Valves: MOV. — Fails To Operate	1×10^{-3}/D	3×10^{-4} 3×10^{-3}	1×10^{-3}	1×10^{-2}	2×10^{-3}	7×10^{-2}	2×10^{-4}			NA	1×10^{-2}	1×10^{-3}	3×10^{-3}	3×10^{-3}	2×10^{-3}	NA	1×10^{-3}	NA	2×10^{-3}	NA	NA	3×10^{-3}	1×10^{-3}	NA	NA	NA	NA	NA	1×10^{-3}	2×10^{-3}	2×10^{-4}
	Valves: MOV. — (Plug) Failure To Remain Open	1×10^{-4}/D	3×10^{-5} 3×10^{-4}	3×10^{-5}/D		NA	3×10^{-4}				NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA	NA	NA	NA	NA	NA	6×10^{-6}		NA
	External Leak Or Rupture	1×10^{-9}/HR	1×10^{-9} 1×10^{-7}	3×10^{-8}		NA					NA		1×10^{-8}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-8}
	Valves (SOV) — Fails To Operate	1×10^{-3}/D	3×10^{-4} 3×10^{-3}	1×10^{-3}		1×10^{-3}					NA	2×10^{-5}	4×10^{-6}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	2×10^{-5}	NA	NA	NA	NA	NA	NA	6×10^{-3} 1×10^{-2} 1×10^{-3}		1×10^{-4}
	Valves (AOV) — Fails To Operate	3×10^{-4}/D	1×10^{-4} 1×10^{-3}	1×10^{-4}	4×10^{-4}	4×10^{-4}					NA	2×10^{-2}	7×10^{-4}	1×10^{-3}	4×10^{-4}	2×10^{-5}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-6}
	Valves (AOV) — (Plug) Failure To Remain Open	1×10^{-4}/D	3×10^{-5} 3×10^{-4}	3×10^{-5}/D		NA	3×10^{-4}				NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	3×10^{-6}
	External Leak — Rupture	1×10^{-9}/HR	1×10^{-9} 1×10^{-7}	3×10^{-8}		NA					NA		1×10^{-8}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
	Valves (Check) — Failure To Open	1×10^{-4}/D	3×10^{-5} 3×10^{-4}	1×10^{-4}	2×10^{-5}	3×10^{-4}	3×10^{-5}	2×10^{-4}			NA		3×10^{-5}	NA	3×10^{-5}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	3×10^{-5}		3×10^{-5}
	Valves (Check) — Reverse Leak	3×10^{-7}/HR	1×10^{-7} 1×10^{-6}		2×10^{-7}	1×10^{-6}	1×10^{-7}	9×10^{-7}			NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
	External Leak — Rupture	1×10^{-9}/HR	1×10^{-9} 1×10^{-7}	3×10^{-8}		NA	1×10^{-6}				NA		1×10^{-8}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-8}
	Valves (Vacuum) — Failure To Operate	3×10^{-5}/D	1×10^{-5} 1×10^{-4}		1×10^{-5}	1×10^{-4}		7×10^{-5}			NA		1×10^{-5}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-5}		NA
	Valves (Vacuum) — Rupture	1×10^{-6}/HR	1×10^{-9} 1×10^{-7}			2×10^{-9}					NA		NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-9}
	Valves: Orifices, Pipe Rupture (Total)	1×10^{-6}/HR	1×10^{-9} 1×10^{-7}			NA					NA		1×10^{-8}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	6×10^{-8}		NA
	Valves (Manual) — Failure To Remain Open (Plug)	1×10^{-4}/D	3×10^{-5} 3×10^{-4}	3×10^{-5}/D		NA	3×10^{-4}				NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	Valves (Relief) — Fail To Open/D	1×10^{-5}/D	3×10^{-6} 3×10^{-5}	1×10^{-5}		3.6×10^{-5}		1.4×10^{-5}																									1×10^{-5}
	Valves (Relief) — Premature Open/HR	1×10^{-5}/HR	3×10^{-6} 3×10^{-5}	1×10^{-5}		1.4×10^{-6}		1.4×10^{-5}																									1×10^{-5}
	Pipes > 3" Nt Quality — Rupture (Section)	1×10^{-10}/HR	3×10^{-12} 3×10^{-9}	1×10^{-10}		NA	5×10^{-8}	2×10^{-9}	1×10^{-10}	1×10^{-8}	7×10^{-8}		1×10^{-8}	NA	2×10^{-10}	3×10^{-9}	NA	NA	NA	NA	1×10^{-8}	1×10^{-8}	NA	6×10^{-9}	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-8}/HR
	Pipes < 3" — Rupture	1×10^{-9}/HR	3×10^{-11} 3×10^{-8}	1×10^{-9}		NA	5×10^{-8}	2×10^{-9}					1×10^{-8}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-8}/HR
	Gaskets — Leak	3×10^{-6}/HR	1×10^{-7} 1×10^{-4}	1×10^{-6}	1×10^{-7}	3×10^{-6}		9×10^{-7}		1×10^{-7}	NA		NA	6×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	NA	5×10^{-7}	NA	NA	NA	NA	NA	NA	NA		2×10^{-6}	
	Flanges, Closures, — Leak/Rupture Elbows:	3×10^{-7}/HR	1×10^{-8} 1×10^{-5}							3×10^{-8}	NA		1×10^{-6}	1×10^{-6}	2×10^{-8}	NA	NA	NA	NA	NA	NA	NA	2×10^{-7}	2×10^{-7}	NA	NA	NA	NA	NA	NA	NA		2×10^{-8}	
	Welds — Leak	3×10^{-9}/HR	1×10^{-10} 1×10^{-7}								4×10^{-6} 4×10^{-8}		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-7}
	Diesel (Complete Plant) (Emergency Loads) — Failure to Start Oil:	3×10^{-2}/D	1×10^{-2} 1×10^{-1}	3×10^{-2}		NA	1×10^{-3}	1×10^{-1}					NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-5}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-8}
	Diesel (Complete Plant) (Emergency Loads) — Failure to Run 1.0	3×10^{-3}/HR	3×10^{-4} 3×10^{-2}	7×10^{-3}		NA							NA	1×10^{-3}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-4}
	Diesel (Engine Only) — Failure to Run 1.0	3×10^{-4}/HR	3×10^{-5} 3×10^{-3}			NA		1×10^{-3}					NA	1×10^{-3}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-4}
	Batteries — Power Supplies NO/Output 3.0	3×10^{-6}/HR	1×10^{-6} 1×10^{-5}	3×10^{-7}	1×10^{-6}	3×10^{-6}		2×10^{-7}					6×10^{-6}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-7}
	Instrumentation Channels (Amplifiers, Annunciators, Transducers, Combinations) — Failure to Operate 1.5	1×10^{-6}/HR	1×10^{-7} 1×10^{-5}	1×10^{-6}	3×10^{-6}	3×10^{-7}	3×10^{-7}	5×10^{-5} 5×10^{-6}				6×10^{-7}	4×10^{-5}	6×10^{-7}	1×10^{-6}	6×10^{-5}	NA	NA	3×10^{-5}	8×10^{-7}	8×10^{-6}	8×10^{-7}	NA	NA	7×10^{-7}	NA	NA	NA	5×10^{-5}	2×10^{-5}	NA	NA	6×10^{-7}
	Instrumentation Channels (Amplifiers, Annunciators, Transducers, Combinations) — Shift Calibration 2.0	3×10^{-5}/HR	3×10^{-6} 3×10^{-4}			1×10^{-4}							NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-3}

Table III 2-1 (Sheet 1 of 2)

TABLE III 2-1 (Continued)

		ASSESSMENT MEDIAN	LOWER & UPPER BOUND	US NUC OPERATING EXPERIENCE 1,2	AVCO 6	FARADA 5	LMEC 7	SRS 4	COLLINS NUC 8	HOLMES HR-1RD 9	PIONEER 20	CHEM UNCERTAIN UK-CHEM 10,11	SHORE UK-NUC 34	BOURNE UK 35	UNDERAKES GERMAN 36	DAVIL 37	EUROPE NUC AGENCY 38	PUGH 39	STEWAR UK CHEM 40	MOORE 41	IEEE TRANS UK-NUC 42a	IEEE TRANS GER 42b	BOURNE UK 43	OTWAY 44	FARMER UK GAS 45	BEATTIE 46	BEN 47	SPEIT TV 48	HEADINGTON 49	GULF 50	PROCEEDING 51	EEI 3	NRTS IDAHO 52
FAILURE MODES	CLUTCH ELEC — Failure to Operate	3×10^{-4}/D	$1\times10^{-4}-1\times10^{-3}$	3×10^{-4}	2×10^{-4}	4×10^{-3}		2×10^{-3}		1×10^{-4}	NA		NA	4×10^{-3}	NA	NA	NA	NA	1×10^{-4}	NA	NA	1×10^{-3}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-4}
	CLUTCH ELEC — Premature Open	1×10^{-6}/HR	$1\times10^{-7}-1\times10^{-5}$	NA	2×10^{-7}	3×10^{-6}		2×10^{-6}		6×10^{-7}	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	4×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA
	CLUTCH MECH — Failure to Open	3×10^{-7}/HR	$3\times10^{-8}-3\times10^{-6}$		2×10^{-8}	3×10^{-7}		2×10^{-7}		6×10^{-8}	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA
	CLUTCH MECH — Failure to Operate	3×10^{-4}/D	$1\times10^{-4}-1\times10^{-3}$	3×10^{-4}	1×10^{-4}	4×10^{-3}		1×10^{-3}		1×10^{-4}	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA
	SCRAM RODS — Failure to Insert (Single Rod)	1×10^{-4}/D	$3\times10^{-5}-3\times10^{-4}$	$5\times10^{-5}-3\times10^{-4}$/D	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	ELECTRIC MOTORS — Failure to Start	3×10^{-4}/D	$1\times10^{-4}-1\times10^{-3}$	3×10^{-4}/D	1×10^{-3}	7×10^{-5}	3×10^{-3}	1×10^{-4}		1×10^{-4}	NA		2×10^{-4}	1×10^{-3}	4×10^{-4}	1×10^{-3}	4×10^{-4}	NA	NA	NA	NA	1×10^{-4}	NA	2×10^{-4}	NA	NA	NA	NA	NA	NA	1×10^{-4}		3×10^{-4}	2×10^{-4}
	ELECTRIC MOTORS — Failure to Run	1×10^{-5}/HR	$3\times10^{-6}-3\times10^{-5}$	1×10^{-6}/HR	2×10^{-6}	2×10^{-5}	1×10^{-4}	2×10^{-5}		8×10^{-7}	NA		6×10^{-6}	2×10^{-5}	1×10^{-5}	3×10^{-6}	1×10^{-5}	NA	NA	NA	NA	NA	NA	NA	5×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	8×10^{-7}	1×10^{-5}
	Failure to Run (Extreme ENVIR)	1×10^{-3}/HR	$1\times10^{-4}-1\times10^{-2}$	NA		1×10^{-4}	1×10^{-3}			3×10^{-2}	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA
	RELAYS — Failure to Energize	1×10^{-4}/D	$3\times10^{-5}-3\times10^{-4}$	3×10^{-5}/D	1×10^{-4}	1×10^{-4}	4×10^{-4}	5×10^{-4}		9×10^{-5}	NA		2×10^{-4}	1×10^{-5}	NA	NA	4×10^{-4}	NA	1×10^{-4}	1×10^{-4}	1×10^{-3}	3×10^{-4}	1×10^{-4}	NA	NA	NA	NA	4×10^{-5}	3×10^{-4}	1×10^{-3}	NA	NA		2×10^{-4}
	RELAYS — Failure NO Contact to Close	3×10^{-7} HR	$1\times10^{-7}-1\times10^{-6}$	1×10^{-6}/HR	5×10^{-7}	4×10^{-6}				2×10^{-7}	NA		NA	2×10^{-7}	1×10^{-7}	NA	NA	NA	2×10^{-7}	3×10^{-7}	NA	2×10^{-6}	3×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	NA		6×10^{-7}
	RELAYS — Short Across NO/NC Contact	1×10^{-8}/HR	$1\times10^{-9}-1\times10^{-7}$	1×10^{-6}/HR		1×10^{-7}				2×10^{-7}	NA		NA	NA	2×10^{-7}	NA	NA	NA	NA	NA	NA	NA	1×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-7}
	RELAYS — Open NC Contact	1×10^{-7} HR	$3\times10^{-8}-3\times10^{-7}$	1×10^{-6}/HR						NA	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-6}	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-6}
	SWITCHES — Limit: Failure to Operate	3×10^{-4}/D	$1\times10^{-4}-1\times10^{-3}$	1×10^{-4}/D		3×10^{-4}		7×10^{-4}		1×10^{-4}	NA		1×10^{-4}	NA	NA	NA	NA	NA	7×10^{-4}	NA	NA	NA	4×10^{-4}	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-3}
	SWITCHES — Torque: Fail to OPER	1×10^{-4}/D	$3\times10^{-5}-3\times10^{-4}$	1×10^{-4}		1×10^{-4}				NA	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		2×10^{-6}
	SWITCHES — Pressure Fail to OPER	1×10^{-4}/D	$3\times10^{-5}-3\times10^{-4}$	1×10^{-4}	5×10^{-5}	1×10^{-3}				NA	NA	1×10^{-3}/D	NA	5×10^{-3}	NA	NA	NA	NA	1×10^{-3}/D	1×10^{-3}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-3}	NA		1×10^{-4}
	SWITCHES — Manual, Fail to TRANS	1×10^{-5}/D	$3\times10^{-6}-3\times10^{-5}$	3×10^{-5}	3×10^{-6}	5×10^{-4}	7×10^{-5}	1×10^{-4}		2×10^{-5}	NA		2×10^{-4}	7×10^{-4}	1×10^{-4}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-4}	NA		7×10^{-5}		2×10^{-4}/D
	SWITCHES — Contacts Short	1×10^{-8}/HR	$1\times10^{-8}-1\times10^{-7}$	3×10^{-8}		5×10^{-7}				5×10^{-7}	NA		NA	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	3×10^{-6}	NA	NA	NA		
	CIRCUIT BREAKERS — Failure to Operate	1×10^{-3}/D	$3\times10^{-4}-3\times10^{-3}$	1×10^{-3}/D	1×10^{-4}	3×10^{-4}		2×10^{-3}		1×10^{-4}	NA		1×10^{-3}	3×10^{-3}	4×10^{-4}	7×10^{-5}	8×10^{-5}	NA	NA	NA	1×10^{-3}	2×10^{-4}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		2×10^{-5}/D
	CIRCUIT BREAKERS — Premature Operate	1×10^{-6}/HR	$3\times10^{-7}-3\times10^{-6}$	1×10^{-6}/HR	3×10^{-7}	1×10^{-6}		6×10^{-6}		3×10^{-7}	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	5×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA			
	FUSES — Premature, Open	1×10^{-6}/HR	$3\times10^{-7}-3\times10^{-6}$	NA	5×10^{-7}	4×10^{-6}				5×10^{-7}	NA		3×10^{-6}	5×10^{-6}	NA	NA	NA	NA	NA	NA	NA	2×10^{-7}	NA	NA	NA	NA	NA	NA	1×10^{-6}	NA	NA	NA		4×10^{-6}
	FUSES — Failure to Open	1×10^{-5}/D	$3\times10^{-6}-3\times10^{-5}$	1×10^{-6}/D		1×10^{-5}				5×10^{-7}	NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	7×10^{-5}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA
	WIRES — Open	3×10^{-7}/HR	$1\times10^{-6}-1\times10^{-5}$	1×10^{-6}/HR		2×10^{-6}					NA		2×10^{-6}	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-7}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-4}
	WIRES — Short to GND	3×10^{-7}/HR	$3\times10^{-9}-3\times10^{-6}$	1×10^{-7}/HR		1×10^{-6}					NA		1×10^{-6}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	3×10^{-10}	NA	NA	NA		1×10^{-7}
	WIRES — Short to PWR	1×10^{-8}/HR	$1\times10^{-9}-1\times10^{-7}$			1×10^{-7}					NA		1×10^{-6}	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-7}
	TRANSFORMERS — Open CKT	1×10^{-6}/HR	$3\times10^{-7}-3\times10^{-6}$	1×10^{-6}		1×10^{-6}				1×10^{-6}	NA		NA	NA	NA	NA	NA	NA	3×10^{-7}	NA	NA	1×10^{-6}	NA	NA	NA	NA	NA	NA	2×10^{-7}	NA	NA	NA	1×10^{-6}	1×10^{-7}
	TRANSFORMERS — Short	1×10^{-6}/HR	$3\times10^{-7}-3\times10^{-6}$	1×10^{-6}		1×10^{-6}				1×10^{-6}	NA		NA	NA	NA	NA	NA	NA	3×10^{-7}	NA	NA	1×10^{-6}	NA	NA	NA	NA	NA	NA	1×10^{-6}	NA	NA	NA	1×10^{-6}	2×10^{-7}/HR
	SOLID STATE DEVICES — Fails to Function	3×10^{-6}/HR	$3\times10^{-7}-3\times10^{-5}$	1×10^{-6}/HR		2×10^{-6}					NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		1×10^{-4}/HR
	SOLID STATE DEVICES — Hi PWR Application Shorts	1×10^{-6}/HR	$1\times10^{-7}-1\times10^{-5}$	1×10^{-7}/HR		1×10^{-6}					NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		NA
	SOLID STATE DEVICES — Fails To Function Low PWR Application	1×10^{-6}/HR	$1\times10^{-7}-1\times10^{-5}$	1×10^{-7}/HR		2×10^{-6}					NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	2×10^{-7}	NA	NA		NA
	SOLID STATE DEVICES — Shorts	1×10^{-7}/HR	$1\times10^{-8}-1\times10^{-6}$			1×10^{-6}					NA		NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	1×10^{-7}	NA	NA		

Table III 2-1 (Sheet 2 of 2)

TABLE III 2-2 COMPARISON OF ASSESSMENTS WITH NUCLEAR EXPERIENCE

Component/Primary Failure Modes	Assessed Values		Nuclear Experience[a]
	Lower Bound	Upper Bound	
Mechanical Hardware			
Pumps			
Failure to start, Q_d:	3×10^{-4}/d	3×10^{-3}/d	1×10^{-3}/d
Failure to run, λ_o: (Normal Environments)	3×10^{-6}/hr	3×10^{-4}/hr	3×10^{-6}/hr[b]
Valves			
Motor Operated			
Failure to operate, Q_d:	3×10^{-4}/d	3×10^{-3}/d	1×10^{-3}/d
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d	3×10^{-5}/d[c]
Solenoid Operated			
Failure to operate, Q_d:	3×10^{-4}/d	3×10^{-3}/d	1×10^{-3}
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d	3×10^{-5}/d[c]
Air Operated			
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-3}/d	1×10^{-4}/d
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d	3×10^{-5}/d[c]
Check			
Failure to open, Q_d:	3×10^{-5}/d	3×10^{-4}/d	1×10^{-4}/d
Relief			
Failure to open, Q_d:	3×10^{-6}/d	3×10^{-5}/d	1×10^{-5}/d
Manual			
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d	3×10^{-5}/d
Pipe			
Plug/rupture			
$\leq$ 3" diameter, λ_o:	3×10^{-11}/hr	3×10^{-8}/hr	1×10^{-9}/hr
> 3" diameter, λ_o:	3×10^{-12}/hr	3×10^{-9}/hr	1×10^{-10}/hr
Clutches			
Mechanical			
Failure to engage/ disengage	1×10^{-4}/d	1×10^{-3}/d	3×10^{-4}/d
Electrical Hardware			
Electrical Clutches			
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-3}/d	3×10^{-4}/d

TABLE III 2-2 (Continued)

Component/Primary Failure Modes	Assessed Values		Nuclear Experience[a]
	Lower Bound	Upper Bound	
Motors			
Failure to start, Q_d:	1×10^{-4}/d	1×10^{-3}/d	3×10^{-4}/d
Failure to run (Normal Environments), λ_o:	3×10^{-6}/hr	3×10^{-5}/hr	1×10^{-6}/hr[d]
Transformers			
Open/shorts, λ_o:	3×10^{-7}/hr	3×10^{-6}/hr	1×10^{-6}/hr
Relays			
Failure to energize, Q_d:	3×10^{-5}/d	3×10^{-4}/d	3×10^{-5}/d
Circuit Breaker			
Failure to transfer, Q_d:	3×10^{-4}/d	3×10^{-3}/d	1×10^{-3}/d
Limit Switches			
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-3}/d	1×10^{-4}/d
Torque Switches			
Failure to operate, Q_d:	3×10^{-5}/d	3×10^{-4}/d	1×10^{-4}/d
Pressure Switches			
Failure to operate, Q_d:	3×10^{-5}/d	3×10^{-4}/d	1×10^{-4}/d
Manual Switches			
Failure to operate, Q_d:	3×10^{-6}/d	3×10^{-5}/d	3×10^{-5}/d
Battery Power Supplies			
Failure to provide proper output, λ_s:	1×10^{-6}/hr	1×10^{-5}/hr	3×10^{-7}/hr[e]
Solid State Devices			
Fails to function, λ_o:	3×10^{-7}/hr	3×10^{-5}/hr	1×10^{-6}/hr
Diesels (complete plant)			
Failure to start, Q_d:	1×10^{-2}/d	1×10^{-1}/d	3×10^{-2}/d
Failure to run, λ_o:	3×10^{-4}/hr	3×10^{-2}/hr	1×10^{-3}/hr
Instrumentation			
Failure to operate λ_o:	1×10^{-7}/hr	1×10^{-5}/hr	1×10^{-6}/hr

(a) All values are rounded to the nearest half order of magnitude on the exponent.

(b) Derived from averaged data on pumps, combining standby and operate time.

(c) Approximated from plugging that was detected.

(d) Derived from combined standby and operate data.

(e) Derived from standby test on batteries, which does not include load.

TABLE III 2-3 COMPARISON OF ASSESSMENTS WITH INDUSTRIAL EXPERIENCE

Component/Primary Failure Modes	Active Mechanical Hardware			
	Lower Bounds		Upper Bounds	
	Assessed	Industrial[a]	Assessed	Industrial[a]
Pumps				
Failure to start, Q_d:	3×10^{-4}/d	5×10^{-5}/d	3×10^{-3}/d	5×10^{-3}/d
Failure to run, λ_o: (Normal Environments)	3×10^{-6}/hr	1×10^{-7}/hr	3×10^{-4}/hr	1×10^{-4}/hr
Failure to run, λ_o: (Extreme Environment)	1×10^{-4}/hr	1×10^{-4}/hr	1×10^{-2}/hr	1×10^{-3}/hr
Valves				
Motor Operated				
Failure to operate, Q_d:	3×10^{-4}/d	2×10^{-4}/d	3×10^{-3}/d	7×10^{-2}/d[b]
Plugs, Q_d:	3×10^{-5}/d	6×10^{-5}/d[a]	3×10^{-4}/d	3×10^{-4}/d[a]
Solenoid Operated				
Failure to operate, Q_d:	3×10^{-4}/d	2×10^{-5}/d	3×10^{-3}/d	6×10^{-3}/d
Air Operated				
Failure to Operate, Q_d:	1×10^{-4}/d	1×10^{-6}/d	1×10^{-3}/d	2×10^{-2}/d[c]
Check				
Failure to open, Q_d:	3×10^{-5}/d	2×10^{-5}/d	3×10^{-4}/d	3×10^{-4}/d
Reverse leak, λ_o:	1×10^{-7}/hr	1×10^{-7}/hr	1×10^{-6}/hr	1×10^{-6}/hr
Vacuum				
Failure to operate, Q_d:	1×10^{-5}/d	1×10^{-5}/d	1×10^{-4}/d	1×10^{-4}/d
Relief				
Failure to open, Q_d:	3×10^{-6}/d	1.4×10^{-5}/d	3×10^{-5}/d	3.6×10^{-5}/d
Manual				
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d[d]	3×10^{-4}/d	3×10^{-4}/d[d]
Pipe				
Plug/rupture, λ_o:				
≤ 3" diameter	3×10^{-11}/hr	2×10^{-9}/hr	3×10^{-8}/hr	5×10^{-6}/hr[e]
> 3" diameter	3×10^{-12}/hr	1×10^{-10}/hr	3×10^{-9}/hr	5×10^{-6}/hr[e]
Clutches				
Mechanical				
Failure to engage/ disengage, Q_d:	1×10^{-4}/d	1×10^{-4}/d	1×10^{-3}/d	4×10^{-3}/d

TABLE III 2-3 (Continued)

Component/Primary Failure Modes	Lower Bounds		Upper Bounds	
	Assessed	Industrial[a]	Assessed	Industrial[a]
Clutches, electric				
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-4}/d	1×10^{-3}/d	4×10^{-3}/d
Motors, electric				
Failure to start, Q_d:	1×10^{-4}/d	7×10^{-5}/d	1×10^{-3}/d	3×10^{-3}/d[f]
Failure to run, given start (Normal environments), λ_o:	3×10^{-5}/hr	5×10^{-7}/hr	3×10^{-5}/hr	1×10^{-4}/hr
Failure to run, given start (Extreme Environments), λ_o:	1×10^{-4}/hr	1×10^{-4}/hr	1×10^{-2}/hr	3×10^{-2}/hr
Transformers				
Open/shorts, λ_o:	3×10^{-7}/hr	1×10^{-7}/hr	3×10^{-6}/hr	1×10^{-6}/hr
Relays				
Failure to energize, Q_d:	3×10^{-5}/d	4×10^{-5}/d	3×10^{-4}/d	1×10^{-3}/d[g]
Circuit Breakers				
Failure to transfer, Q_d:	3×10^{-4}/d	2×10^{-5}/d	3×10^{-3}/d	3×10^{-3}/d
Limit Switches				
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-5}/d	1×10^{-3}/d	7×10^{-4}/d
Torque Switches				
Failure to operate, Q_d:	3×10^{-5}/d	2×10^{-5}/d	3×10^{-4}/d	1×10^{-4}/d
Pressure Switches				
Failure to operate, Q_d:	3×10^{-5}	5×10^{-5}/d	3×10^{-4}/d	1×10^{-3}/d
Manual Switches				
Failure to transfer, Q_d:	3×10^{-6}/d	3×10^{-6}/d	3×10^{-5}/d	$.7 \times 10^{-4}$/d[h]
Battery Power Supplies				
Failure to provide proper output, λ_s:	1×10^{-6}/hr	1×10^{-7}/hr	1×10^{-5}/hr	6×10^{-6}/hr
Solid State Devices				
Fails to function, λ_o: (Hi power application)	3×10^{-7}/hr	2×10^{-6}/hr	3×10^{-5}/hr	1×10^{-4}/hr[i]
Fails to function, λ_o: (Low power application)	1×10^{-7}/hr	2×10^{-7}/hr	1×10^{-5}/hr	2×10^{-6}/hr

TABLE III 2-3 (Continued)

Component/Primary Failure Modes	Lower Bounds		Upper Bounds	
	Assessed	Industrial[a]	Assessed	Industrial[a]
Diesels				
Failure to start, Q_d:	1×10^{-2}/d	1×10^{-3}/d	1×10^{-1}/d	1×10^{-1}/d
Failure to run, λ_o: (emergency loads)	3×10^{-4}/hr	1×10^{-4}/hr	3×10^{-2}/hr	1×10^{-3}/hr
Instrumentation				
Failure to operate, λ_o:	1×10^{-7}/hr	3×10^{-7}/hr	1×10^{-5}/hr	6×10^{-5}/hr[j]

(a) Some demand values derived from data on continuously operating systems.

(b) Derived for values in high temperature sodium environment.

(c) Includes failures due to improper air supplies.

(d) These values derived from data on continuously operating system; only one industrial source listed this mode.

(e) Due to the varying unit of pipe lengths in the different sources (per foot, per section, per plant, etc.), the failure rates from the industrial sources have extremely wide ranges. For detailed comparison of pipe failure rates see the special assessment section of this appendix.

(f) This value obtained from high temperature liquid metal test reactor applications.

(g) Data from average of all modes of relay failures.

(h) Data from average of all modes of switch failures.

(i) This value derived from experimental reactor experience.

(j) Data from chemical industry.

Section 3

Current Nuclear Experience

3.1 INTRODUCTION

As an input to the range assessments, current, commercial reactor experience was examined for component data. There was a definite problem in obtaining usable data since reactor history has been recorded with little view toward quantitative evaluations. Sufficient quantitative characteristics are not generally recorded for the failure occurrences, there is little categorization and classification for statistical and behavioral (trend) evaluations, and there is little systematic storage of the data for quantitative evaluation and retrieval.

Had more accurate nuclear data been available, the ranges that were assessed in the data base could have had narrower values. Precise detailed component information was not obtainable; instead gross, averaged statistics were estimated. Because of the random variable approach, however, the averaged nuclear statistics could be incorporated as important data for the assessed data ranges.

In the assessment procedure, involving the study's data base, the assessed ranges were compared with the nuclear data values to ensure that the nuclear data were consistent with the defined ranges and that the nuclear values did not contradict the range assessments.

The averaged nuclear data values were obtained by examining operating history of nuclear power plants and manually extracting data estimates, i.e., failure rates and demand probabilities, using standard reliability evaluation techniques. Comparisons of the nuclear data with the assessed ranges have been given in the previous tables. The evaluations performed to obtain the nuclear data values are reviewed in this section. Summarized listings also are provided of the raw data employed in the evaluations. Also given are certain additional trend analyses which were performed in conjunction with the data estimation and which were considered in the range assessments. In addition to the averaged estimations that were performed, which served as the basic data, other investigations were performed in order to check model and data adequacy. These were done on an individual failure level, where actual failure incidents were examined. With regard to the fault tree and event tree models, the incidents were examined to determine if the general failure definitions in the models included such particular occurrences. With regard to the data base, the incidents were examined to see if such mechanisms and causes were given coverage by the total failure rate and demand probabilities and their associated ranges.

The experience examined in these failure investigations included 1971-1973 reactor incident files and operating occurrence reports (including certain pertinent earlier failures), Nuclear Safety Information Center files, environmental reports, National Technical Information Services files, RESPONSA information, individual published reports, and other pertinent sources. These sources are included in the reference and bibliography listings given in this appendix, with brief summaries of their use. A tabulated listing is given at the end of this section to show the nature of the investigations performed and the considerations undertaken.

3.2 NUCLEAR EXPERIENCE STATISTICS

Since experience history tended to be more quantitatively deficient the earlier it was recorded, recent 1972-73 experience was examined for the sample estimates of averaged statistics. In particular, the one year period from Jan. 1, 1972 through December 31, 1972 was used to evaluate the summarized and averaged nuclear data statistics, which in turn were used in the range comparisons and consistency checks. Preliminary analysis of the experience, consisting of the period in 1973 to date, gave no gross differences compared to the one year period sample.

In addition to the averaged statistical evaluation, detailed nuclear history, including experience earlier than 1972, was examined on an individual failure level. As stated, the failure analysis served as a check on the fault tree models and event tree models which had been constructed. Analysis of the failure modes also served to check the adequacy of the failure rates and demand

probabilities which had been definite. At the end of this section, a tabulated listing is given summarizing the investigations which were done.

The tables which follow are self-explanatory. The 1972 experience, used for the statistical analyses, was obtained from the listings which have been recently assembled by the Directorate of Regulatory Operations, Office of Operations Evaluation. The data listed are those reported by the utilities in accordance with Regulatory Guide 1.6 and the Technical Specifications in the AEC license for the applicable reactors.

For the 1972 time period, a total of approximately 700 failures and anomalies were reported. Because of the constant failure rate assumption, consideration was restricted to those plants which had operated for the entire one year period. Also, only those failures which were relevant to the data base categorizations were considered (i.e. safety related failures). The total number of failures and anomalies evaluated was then reduced to 303.

Table III 3-1 lists the 17 plants which were operational for the 1972 one year period and which formed the data base for the evaluations. Of the 17 plants, 8 were pressurized water reactors (PWR) and 9 were boiling water reactors (BWR). The table lists the number of failures occurring, subcategorized into those occurring while the plant was in standby status and in operation status. The operating times have been rounded to one year, which is sufficient for the accuracies being considered.

Table III 3-2 categorizes the 303 failures into generic component classes and exemplifies the type of categorizaton that was performed to obtain statistical estimates of averaged failure rates and demand probabilities. For these statistical estimates, further detailed subclassifications were not performed since the accompanying details were masked by the basic data uncertainties and were covered in the assessed ranges.

The averaged (standby) failure rate estimates were obtained by using the standard equation, in applicable form here:

$$\lambda_s = \frac{n_f}{N_p N_c T}$$

where

n_f = number of failures observed

N_p = number of plants (17)

N_c = average number of components per plant

T = observed (standby) time period (8760 hr)

Since safety systems were examined, N_c is thus in general the average number of components associated with the safety systems in an individual plant. For each class of failure, N_c was estimated based on average plant statistics which constituted sufficient accuracy with regard to data resolution and assessed range widths.

Instead of failure rates, the failure statistics can also be expressed in terms of failure upon demand probabilities (or simply demand probabilities), Q_d, which were obtained by using the standard binomial estimate,

$$Q_d = \frac{n_f}{N_p N_c N_T}$$

where N_p and N_c are as defined previously and N_T is the average number of tests (demands) performed per component per year. (The averaged demand probability has an additional factor of 0.5. Because of the half-exponent rounding procedure, this was not included.)

Tables III 3-3 and III 3-4 give the failure rates and demand probabilities for pumps, piping, control rods, diesels, and valves, using the above formulas and the summarized failure statistics in Table III 3-2. Standard procedures, such as chi-square evaluations, can be used to obtain approximate confidence bounds on the component estimates. Such bounds at 90% were in general of the order of a factor of 3 to 10 in width. These bounds are not particularly pertinent nor applicable since they represent the spread on the averaged estimate and do not account for the errors due to the averaging process itself (i.e., lumping failures of different modes, different component pedigrees, etc.).[1]

---

[1] It should be noted that these bounds are classical, confidence bounds and are not random variable related (i.e. for the classical bounds, the data are treated as parameters and not random variables).

The estimates in Tables III 3-3 and III 3-4 have been rounded to the nearest half exponent to conform with the assessment scale used in the study (i.e., $10^{-1.5}$ or 10^{-1}, etc. giving 1 or 3 as a significant figure for the failure rates and demand probabilities). At the end of this section is a tabulated listing of the failures used to obtain the various averaged nuclear estimates which served as input to the assessed ranges. (The failures were also part of those examined on an individual level for model checking).

In addition to the averaged estimates, nuclear operating experience was used to check relative orderings of the assessed ranges (highest failure rate, second highest, etc.). This ordering check aided in determining whether the component failure rates were properly assessed on a relative scale.

The relative ordering investigations entailed an ordering of nuclear estimates and then comparing this ordering with the ordering of the study's assessed ranges. The data used were those in Table III 3-2 and those listed at the end of this section. Checks were made on recent 1973 experience, revealing no significant changes from the data already used. With regard to absolute failure occurrences from the nuclear history, valves dominated, contributing 34% of the failures followed by instrumentation 16%, pumps 8%, control rods (all failures) 8% and diesel generators 7%. Miscellaneous and human failures formed the remaining contribution. These statistics were in general agreement with those obtained from the assessed ranges and fault tree results.[1]

Finally, with regard to nuclear experience statistics, common mode surveys were performed to investigate component failure and dependencies in order to gain additional perspective on the adequacy of the models and coverages given to common mode effects. The surveys performed here served as checks on the common mode treatments of component failures including the quantitative coverages given. (More details on the model treatments are given in Appendix IV.)

---

[1] More formally, from a statistical point of view and when statistical tests were performed, the nuclear data did not contradict (reject) the model results and data assessment values.

Common mode failures, which involve common causes, can be categorized in a number of ways. One such categorization was given by Williams (Ref. 1) and with certain modifications is used here. Four classes can be defined with regard to gross system and component hardware effects:

a. Component Effect - A single failure which causes a group of redundant or similar components to fail.

b. System Effect - A single failure, which can be a single component hardware failure, that causes a defined system or combination of systems to fail (entailing loss of a defined function).

c. Interaction Effect - A single common mode failure or single hardware failure, which causes a protection function to be required and at the same time renders that protection unavailable.

d. Questionable Effect - As in general with data analyses, there is also a fourth class which contains those failures with too little information for specific categorization.

In addition to effects, common mode failures involving common causes can also be categorized with regard to their basic origin.

a. Design and Manufacturing Cause - Failures which are due to defects and errors in design, manufacturing, quality control, etc.

b. Human Cause - Failures which are due to operator errors, testing, and maintenance errors and lack of procedure.

c. Environment Cause - Failures which result from conditions and causes which are environmentally related, such as those beyond design environments.

d. Hardware Cause - Failures which are due to inherent component failures, which may include "infant mortalities" (burn-in failures).

e. Questionable Cause - Failures for which there is insufficient information.

The aforementioned four group and five group categorizations are still somewhat general, and overlappings can therefore exist, perhaps causing problems with

regard to uniquely classifying the failure. However, the categorization is useful in general behavior and trend analyses and when overlapping questions arose, judgement was made on the dominant failure characteristic and the failure was accordingly classified. The classifications and indentifications of common modes have further impreciseness due to data deficiencies; however, the results were deemed sufficient for the general, overview purpose used.

Table III 3-5 shows a breakdown of the 1972 experience into common mode and non-common mode ("random failure") contributions by reactor. In general, of the PWR failures 10.5% were classed as common mode failures and of the total BWR failures, 11.1% were assessed as common mode. Thus approximately 10% of the occurring failures were classified as common mode, and though this number is not precise it indicates an order of magnitude type of contribution.

The breakdown of the common mode failures into the effect and cause categories is given in Table III 3-6. The tabulation of the common mode failures, is provided in the following pages. The code in parentheses beside each failure refers to the assessed effect class (the alphabetic character) and the assessed cause class (the numerical character), where these characters refer to those previously used in the defined classifications.

The following are reported events which were assessed to be common mode or to have high potential for causing common mode effects.

- The high flow isolation switches for the high pressure coolant injection system (HPCIS) drifted above the technical specification limits. These switches were not of the locking type. Installation of locking switches corrected the problem. (A-1)
- All low pressure permissive switches had drifted above technical specification limits. Switches were changed to locking type. (A-1)
- Trip setting for emergency core cooling system (ECCS) was found to be too low because of absence of any type of a locking device. (A-1)
- Flow switches on two low pressure coolant injection system (LPCIS) pumps failed due to breakage of paddles; heavier duty switches installed. (A-5)
- All main steam line high-flow switches failed due to the use of lead-base sealant in switch assembly. (B-5)
- Four flow switches failed because of a jeweled bearing, which supports the torque tube in each, became contaminated; the bearing housing was redesigned. (D-5)
- During the start-up from cold shutdown, fuses in power supplies for IRM channels BD & F were blown; no cause given. (D-5)
- Three LPCIS delta pressure switches drifted out of technical specification requirements (reactor at 100% power). (D-5)
- With reactor at 85% power low-low reactor pressure switches drifted below technical specification limits. (D-5)
- Water hammer in a cross-over line caused tack welds in 11 hangers to break; heavier tack welds were required to correct problem. (D-5)
- Suction and discharge valves to off-gas samples were left closed; the procedure was changed and the valves were altered to make them "locked-open" valves. (D-2)
- Breaker interlock prevented one pump from starting on signal when the other pump breaker is racked out. (A-2)
- Ten valves failed to close following test due to weak "torque switch torsion springs"; the weak springs prevented the contacts to return to a closed position. (D-1)
- Indicating lamps shorted out and actuated circuit breaker in power line to motor and controller; used 24v in lieu of 120v lamps to solve problem. (D-5)
- Two reactor core isolation cooling system (RCICS) valves failed to open due to inability of the 250v dc breaker to pull in. (D-5)
- During testing all four low-low reactor water level sensors were found to be out of adjustment. All had been calibrated by the same person. (C-2)
- During testing of main steam line low pressure switches, all 4 were found

set (and locked) below technical specification limits of 850 psig. (D-2)

- The magnetic mercoid switches for the main condenser vacuum sensors were set too high. Sensing lines and vacuum header piping contained entrapped condensate. (D-5)

- All low pressure switches on main steam line found set below technical specification limits after recent calibration. (D-2)

- Two solenoid operated isolation valves in torus sampling system failed to close on signal. Dust accumulation on valve intervals had caused valve pistons to bind. (D-3)

- The 2" check valves on HPCIS turbine exhaust drain line let water into the drain trap. Loose rust particles caused valve plugs to bind. (D-3)

- The pump start permissive relay failed to energize because the relays used were not designed for 125 dc operation, and the air gap on both relays was too large, requiring excessive pull in voltage to energize relay. (D-5)

- Water dripped into rod control cabinets from main steam generator feedwater flow lines and grounded control power to stationary gripper coil causing rods to drop into core. (A-1)

- With plant at 90% power 3 control rods dropped into core due to failure of a multiplexing thyristor in the movable gripper coil circuit. (D-1)

- Feedwater control valve (valve for loop "C") failed, introducing feedwater transients into primary system which resulted in a low pressure transient, a reactor shut down, and initiation of safety injection system operation. (B-5)

- During pre-operational testing of Turkey Point Unit #4 a design error in Unit #3 caused a simultaneous actuation of Emergency Core Cooling System for both units. (D-1)

- In the emergency core cooling system, a leak in the upper diaphragm of a pilot valve on the nitrogen pressure regulator caused the regulator to close and the redundant regulator could not maintain the overpressure. (C-5)

- Failure of an overpower rod stop and a reactor trip bistable resulted from an incorrectly sized zener diode in the regulated power supply. (D-5)

- Pressurizer level instrumentation; three narrow range level transmitters were incorrectly calibrated. (D-2)

- Six steam generator (SG) blow down isolation valves failed to respond to safety injection system signals. Temporary jumpers had been installed and technician failed to remove them. (D-2)

- Linkages on six solenoid valves that control main steam stop valves were sticking because of dirt accumulation in the area of the plunger on the solenoid. (D-3)

- Zero settings for all narrow gauge pressurizer level transmitters were found 5% below indicated value; the cause not determined, it could be drift or incorrect calibration. (D-5)

- Cracks were found in welded joints of both feedwater lines for steam generators A and B; the investigation is continuing. (B-5)

3.3 1972 OPERATING INCIDENTS USED FOR STATISTICAL ANALYSES AND INDIVIDUAL FAILURE ANALYSIS

Listed on the following pages are one-line summaries of the failures incorporated in the statistical analyses. The figures cover a spectrum of severities; however, all were of sufficient magnitude to warrant reporting as incidents.

a. Control Rods

Control rod (CR) No. 19 failed to fall into core during startup.

CR No. 19 failed to drop fully and CR No. 18 dropped slowly.

CR No. 19 failed to insert fully and subsequent slow insertion time.

CR No. 19 fell from 90" to 24" following plant trip.

CR inspection showed several missing bolts and locking cups.

CR No. 19 hung up at 36" withdrawn due to embrittled spiral pin.

CR No. 20 hung up at 36.5" withdrawn during scram time measurements.

Four CR's dropped 150 steps into core and initiated load runback.

Four CR drives latched at 6" withdrawn due to dirt, broken carbon seals.

Three CR's dropped into core due to multiplexing thyristor.

Three CR's dropped into core due to multiplexing thyristor.

CR drive stopped to 02 position during scram, had to be manually driven in.

CR failed to fully insert due to excessive leakage across stop-piston seals.

CR drive 22-31 automatically scrammed to the 02 position.

CR drive 22-31 seated at 02 position during scram due to excessive leakage across stop-piston seals.

CR drive 22-31 seated at 02 position during scram.

CR drive malfunctioned due to failed seat on stationary face.

CR drive No. 19 malfunctioned due to primary coolant leakage.

CR drive after scram following manual scram apparently due to scored guide tube during CRDM repairs.

CR No. 26 failed to be withdrawn due to open circuit on motor brake wires.

CR failed to stop; replaced 3 CRDM motors and retested fourth.

CR failed to withdraw due to brake dragging.

CR failed to withdraw due to defective brake operation.

b. Diesels

DG No. 3 failed to start on remote signal.

DG failed to start during test.

DG radiator coolant hose tore loose from recirculating heater outlet.

Propane engine-drive generator malfunctioned twice due to dirt in coil.

DG failed to start due to oil on distributor points.

DG failed to start due to oil lube pressure switch setting drift.

DG failed to come up to voltage due to failed exciter armature.

DG malfunctioned due to improperly connected plug at one of the terminals.

DG failed to start twice due to defective air start motors.

DG failed to start due to defective air start motors.

DG startup terminated due to high crankcase pressure.

DG shut down due to high crankcase pressure. DG spurious trip due to high crankcase pressure.

DG spurious trip due to high crankcase pressure.

DG spurious trip due to high crankcase pressure.

DG failed to start due to rust particles restricting bleed orifice in air relay.

DG failed to start due to dirt in pilot valve in the governor assembly.

Output fluctuations of DG due to dirty contacts in droop relay.

DG tripped during hot standby due to loss of fuel supply.

DG failed to take additional load due to mechanical blockage.

DG malfunctioned due to high temperature of engine cooling water.

DG malfunctioned due to failure of the cooling radiator shutters.

c. Instrumentation

Low-flow scram signal failed to trip turbine.

Low-trip settings for condenser vacuum below spec. due to water in sensing line.

Radiation monitor alarm due to unknown causes.

Both neutron-monitoring startup channels failed due to faulty triax cable.

Low-low reactor water level sensors were out of technical specifications (TS).

Line-break sensors hooked up backwards valving "B" isolation condenser into service.

"A" and "B" isolation condensers failed to be activated due to gauge caught up scale.

Air pressure in scram valve pilot header lost due to de-energized backup scram solenoid.

High flow differential pressure switch failed.

Scram-dump-volume level switch failed to actuate high level alarm.

Pressure bistable failed to de-energize due to bad soldered joint.

Two pressure switches for spray injection system (SIS) drifted above TS limit of 350 psig.

Low pressure scram switches in turbine EHC control system drifted below TS limits.

Low pressure switches on main streamline (MSL) found below TS limits.

MSL low pressure switches drifted below TS limits.

MSL low pressure switches trip settings found below TS limits.

Switch in MSIV "hi-flo" circuit rusted shut due to water drainage from room cooler.

Two high pressure scram switch setpoints drifted above TS limits.

Refueling interlock failure due to limit switch failure as a result of misalignment.

RPS relay for No. 2 turbine stop valve failed to de-energize.

Instrumentation for initiation of core spray and LPCIS - admission valves found out of TS limits.

Turbine control valve closure failed to initiate scram for generator-turbine load mismatch due to broken wire at connector to solenoid.

Isolation condenser flow switch out of specification due to drifted set points.

Reactor pressure switches tripped above TS limits.

Reactor-level switch tripped out of TS limits.

High-flux trip from pressure transient caused by plugged filter in the pilot valve.

LPCI low pressure switch switch failed to signal injection permissive.

Water level trip point drifted below TS minimum.

DP switch for high-flow steam supply to isolation condenser failed.

Reactor vessel high-pressure-scram pressure switch tripped above TS limits.

Time-delays in APRM logic tripped above TS limits.

Level trip switch found out of TS limits.

Turbine lockout occurred due to instabilities in the pressure regulator.

Position switch out of adjustment for the clean-up system aux-pump suction valve.

Sensor relay to the logic cabinet of CRD system found inoperable.

High temperature isolation set point drift.

Flow switch torus-to-drywell vacuum breaker failed in untripped condition.

High-flow isolation sensor in main steam line failed.

APRM channels indicated lower than actual core thermal power.

High-flow switch on isolation condenser found over TS limits.

Low-pressure permissive switch set points drifted above TS limits.

High steam-flow switch on isolation condenser above TS limits.

Reactor pressure scram setpoint found drifted out of specifications.

Low-pressure switch for ECCS found greater than TS limits.

Pressure switch on MSLOB below TS limits.

Off-gas monitor set point found in excess of T.S. limits.

Startup pressure channel failed.

d. Valves

Core spray valve CS-11 failed to open due to improper limit switch setting.

Emergency condenser system valves MO-101 and 102 failed to open due to high torque switch settings.

ECCS, SIS nitrogen pressure regulator upper diaphram pilot valve leak.

Air-operated containment isolation valve failed to operate due to the SOV-432 solenoid pilot valve failure.

Emergency condenser condensate return valve motor power supply breaker tripped.

Condensate return valve on emergency condenser failed to operate.

Emergency condenser Limitorque condensate return valve failed to operate.

Containment isolation valve failed to close due to defective solenoid valve SV-4876 in the controller.

Loop "C" feedwater valve faulty.

Discharge valve to the refueling-water storage tank failed due to excessive binding of packing and stem.

Containment isolation valve in fuel pool/reactor drain line to radwaste failed to close due to defective solenoid valve SV-4876.

Recirculation isolation valve failed to open due to over-torquing of clutch shaft.

Containment isolation valve failed to close due to solenoid valve air leakage.

Containment purge exhaust bypass isolation valve air leakage due to cracked yoke.

Containment purge exhaust bypass isolation valve air leakage due to cracked yoke.

Main steam isolation valve (MSIV) leakage due to pilot valve stem misalignment.

Condensate return valve failed to open due to burned out motor.

Main steam isolation valve failure due to AC control unit.

Main steam isolation valve leakage due to pilot valve stem misalignment.

Main steam isolation valve failed to close due to sticking pilot valve.

Electromatic relief valve failed to reset due to foreign material in valve seat.

Main steam isolation valve leaked.

Main steam isolation valve leaked.

Suction recirculation pump valve failed due to inoperable valve operator.

Recirculation system valve leakage due to packing leakage.

Suction recirculation pump valve failed due to damaged valve operator.

MSIV closure due to pressure vessel overfill and relief valve failure.

Safety relief valve relieved below design pressure.

Retainer valve leakage due to damaged disc-retainer and valve-body threads.

Feedwater check valve and air-operated butterfly valve leaked due to worn rubber seats.

HPCI inboard steam isolation valve failed to open.

Air-operated primary containment sample return isolation valve failed to close due to physical binding.

HPCI motor-operated valve failed to open due to valve jamming against seat.

HPCI motor-operated valve failed to open due to burned relay coil.

LPCI valve failed to close due to disconnected wiring.

LPCI valve failed to operate due to tripped thermal valve motor overload breaker.

Main stop valve/control valve slow closure due to broken wire.

Air-operated primary containment sample return isolation valve failed to close due to physical binding on the valves.

No. 1 turbine control valve fast-acting solenoid failed to actuate due to contamination.

Containment isolation valve leaked.

MSIV slow operation due to sticking pilot valve.

Safety valve leakage.

No. 4 turbine control valve fast-acting solenoid failed to actuate.

Inboard isolation valve failed to close due to tripped motor overload breaker.

HPCI electromatic relief valve failed to open.

HPCI steam valve in drywell failed to open during reactor startup.

Isolation condenser valve failed to open due to faulty valve operator.

MSIV in "B" steam line failed due to oil leak in fitting.

Inboard steam-isolation valve failed to close due to tripped breaker.

HPCI electromatic relief valve failed to open due to scored disc.

Vacuum pump suction valve failed to close fully.

No. 4 turbine control valve failed.

LPCI torus spray isolation valve failed to operate due to galling.

Turbine control valve failed to operate due to faulty load-mismatch relay.

Primary containment rubber-seated vent valve leaked due to cracked seat.

Primary containment rubber-seated vent valve leaked due to cracked seat.

Containment sump isolation valve failed to operate due to incorrect mounting.

HPCI valve failed to operate due to broken disk.

MSIV failed to close due to binding in latching mechanism.

Containment sump isolation valve failed to operate.

Containment sump isolation valve failed to operate.

Containment sump isolation valve failed to operate due to air leakage past regulator.

Feedwater control valve erratic operation due to dirt in air supply.

LPCI valve failed to open due to improperly adjusted position switch.

MSL stop control solenoid valve linkages fouled due to dirt.

Power-operated relief valve stuck open.

Diesel generator solenoid pilot valve failed to open due to dirt particles.

MSIV closed completely due to sheared pin in the linkage.

MSIV closed completely due to sheared pin in the linkage.

MSIV closed completely due to sheared pin in the linkage.

Power operated relief valve failed to close due to scored guide.

Stop valve failed due to limit switch setting.

HPIC valve malfunction caused by plastic pipe cap oil hydraulic control system.

HPIC turbine control valve malfunction due to plastic pieces in pilot-valve oil inlet.

HPCI turbine exhaust check valve leaked.

ECCS outboard head spray-isolation valve failed to close due to adjustment.

Stop-check valve failure due to disc rupture.

Containment isolation valve seat leakage.

HPCI outboard steam isolation valve failed to close due to motor failure.

HPCI exhaust check valve disc found separated from valve hinge.

HPCI steam-supply isolation valve failed to close due to packing leakage.

HPCI exhaust check valve disc rupture.

Group I relief valve malfunction.

Outboard main steam drain isolation valve failed to close due to loose mounting screws.

Recirculation pump discharge valve stuck due to damaged threads.

Relief valve "A" failed to reseat due to rust particles lodged across valve orifice.

Relief valve failed to close due to deposits on second-stage piston orifice.

Primary system relief valves replaced due to spring problems.

Safety relief valve failed to operate due to drift in setpoints.

Safety relief valve malfunction.

Torus-to-drywell vacuum-breaker valve problems due to binding in valve operators.

Air-operated vacuum-breaker valve boot seals found depressurized.

Air-operated vacuum-breaker boot seals found depressurized due to excessive clearance between actuating arm and pilot valve.

Low-flow feedwater containment isolation valve leak due to cut seat surface.

Main steam stop valve on SG failed to close due to faulty, motor operator.

Main steam isolation valve on SG failed to open due to short of drive-motor windings.

Main steam stop valve failed to close due to worn gear.

MSIV inoperable due to broken drum on limit switch.

Limitorque valve inoperable due to broken support bearing for gear shaft.

Pump emergency primary makeup system steam-admission valve failure due to linkage.

Relief valve failure in primary make up system.

e. Pipes

Desuperheating water line of the secondary steam system failed due to a crack.

Reactor vent line failure due to leaky fitting of reducer nipple.

Drain line from coil of second stage reheater failed due to cracks at weld edge.

Bent line to MSIV weld failure due to cracks as a result of excessive line motion.

Discharge line of the emergency service water pump failed due to a rubber expansion joint rupture.

Recycle line to the floor drain system leakage due to erosion of the carbon steel elbow.

Small indentations on piping.

Defective fittings on the feedwater flow DP cell.

Hanger tack welds failed as a result of water hammer in the cross-over line.

Atmospheric control system 18" header cracked.

Carbon steel elbow leaked downstream of steam-trap.

f. Pumps

Shaft thread wear on the feedwater oil pump.

Excessive steam leakage past the control slide valve.

Primary coolant leakage due to pump seal leakages.

ECCS core spray pump failed due to circuit breaker binding and burned out check switch contacts.

Fire in oil supply line to turbine driven feedwater pump.

ECCS core spray pump failed due to circuit breaker misalignment and burned out latch-check switch contacts.

ECCS containment-spray pump start failure as a result of corroded breaker contacts.

Pump failed to operate due to faulty interlock.

Pump in SIS loop failed to start due to improper wiring.

LPCI pump failed to start due to intermittent breaker contacts.

Standby sampling pump inoperative due to fouled oil lubricator.

Sample pump tripped prematurely.

Excessive leakage to primary containment due to recirculation pump "A" seal leakage.

Containment spray pump failed to rotate freely due to galled impeller ring.

ECCS pump failure due to faulty pump-start permissive relay.

Standby liquid control pump failed to develop sufficient head.

Residual heat removal system (RHR) pump failure due to ground fault by air deflector.

RHR pump failure due to upper gland seal overtightness.

Standby liquid control pump failed to develop sufficient head.

Sample pump tripped due to personnel error.

Feedwater pump failure due to overheating of hydrostatic bearings.

Charging pump secured due to crack in socket weld.

Recirculation pump failed due to seal leak.

Sample pump "A" removed from service due to faulty motor leads.

3.4 INDIVIDUAL FAILURE ANALYSIS LISTING

Listed here are investigations and considerations that were given to incidents that have occurred in nuclear operating experience. The tabulations are a sample and serve to illustrate the type of analyses that were performed in checking the fault trees and calculations against actual, individual failure experience. In contrast to the previous statistical analysis of the incidents, the incidents in this phase of the analysis were examined in a more individual engineering manner for model checking purposes.

1. Connecticut Yankee Atomic Power Co. (Connecticut Yankee) #96

   a. Problem. During a routine operation inspection several seismic support hold-down bolts on the sliding supports for the steam generators were loose. Subsequent investigation found eight bolts broken and fifteen others suspected of being broken. There are a total of 256 hold-down bolts on the four steam generators.

      As noted by the incident report this is the second instance of significant bolt failure relative to seismic supports.

   b. Reactor Safety Study (RSS) Action. Questions related to the adequacy of the seismic design for Category 1 structure systems and components were investigated by the study on a sample basis. The results of this work are reported in Appendix X.

2. Consolidated Edison Co. (Indian Point 2) #49

   a. Problem. Eight anchor bolts failed in tension and 120° of the weld which joins the roof dome to the tank wall of the condensate storage tank failed. This tank provides the source

of make up water to the secondary system. At the time of failure the tank contained more than 31,000 gallons but less than 80,000 gallons of water. (Design capacity is 600,000 gallons). Ambient temperature was 20° to 25°F and the wind was from the east to southeast with heavy gusts up to 35 MPH.

b. RSS Action. Consideration of passive failures of the condensate tank and supply lines to the auxiliary feed system has been given in fault tree analysis of the auxiliary feed system.

3. Duke Power Co. (Oconee) #51

a. Problem. Twenty-one of the fifty-two inconel in-core instrument stub tubes (0.75 inch-ID schedule 160) that penetrate the bottom of the reactor vessel broke off inside the vessel. The break occurred in the vicinity of the weld that joins the stub tube to the bottom of the vessel. One additional stub tube had failed at the same location but was not completely sheared. Five additional tubes had failed in the vicinity of the flow distributor plate and several others were bent at a point 2-3 inches above the seal weld. In addition a thermocouple guide extending from the top vessel head had failed and one accelerometer used in measuring vibration had become detached.

Pieces of the failed stub tubes were found throughout the reactor coolant system, ranging in size from small buckshot to pieces approximately 2" in diameter. This caused extensive damage to the tube sheet and tubes in steam generator "A" and lesser damage to the tubes projecting above the tube sheet in generator "B".

b. RSS Action. Failure of the in-core tubes caused loose parts to occur within the reactor coolant system (RCS). In this particular case, which involved the first of a line of vendor plants, the hydraulic design deficiencies were found in initial plant operations and corrected. The occurrence of loose parts within the RCS could potentially result in some flow blockage within the core and cause fuels to overheat. As noted in Appendix I, the study gave consideration to potential consequences resulting from flow blockage.

4. Rochester Gas & Electric Co. (Ginna) #53

a. Problem. Dynamic stress analyses of the pressurizer safety valve installation in the primary system indicate higher reaction forces during safety valve discharge than originally considered, preventing isolation in the event of a failure. The analyses also indicate that an overstressed condition would exist on virtually all of the 3" and 4" pipe and fittings between the pressurizer nozzles and the safety valves.

b. RSS Action. The PWR event trees for small LOCA:

- Specifically recognize the failure possibility of safety valve headers, inadvertently stuck open safety valves and relief valves.
- Specifically define combinations of safety features (ECCS) that would be required to operate in case of the pressurizer vapor space LOCA.
- Have numerical estimates on the failure probability for such ECCS combinations as would be required for the vapor space LOCA, since such a LOCA could cause unique ECCS actuation characteristics which are also recognized and considered in the RSS event trees.

5. Consumer Power Co. (Palisades) #55

a. Problem. During inspection of the primary side of Steam Generator "B" a foreign object believed to be the head and shoulder of one of the bolts which lock the ring shim in the upper guide structure assembly was found. The bolts were 304 SS 2 1/4" long with a nominal 1/2" thread and a 3/4" x 1" shoulder. Preliminary metallurgical examination indicates the failure mechanism as fatigue.

b. RSS Action. Refer to previous comment on item 3 (incident 51).

6. Consolidated Edison Co. (Indian Point 2) #57 and #59

a. Problem. Mechanical binding of three control rods during testing at operating temperature conditions were experienced. Apparent cause of this incident is attributed to a guide sheath undersized condition. Boroscopic examination revealed evidence of scratching, metal galling and conditions that have the appearance of weld splatter.

b. RSS Action. This type of failure contributed to the data base for control rod failures. The fault trees also identify mechanical binding as a possible failure mode for components where appropriate.

7. Virginia Electric Power Co. (Surry-1) #63

a. Problem. While attempting to control the reactor primary coolant temperature by venting steam from the secondary side of the steam generators to the atmosphere, the operator attempted to open the three atmosphere steam power relief valves; however these valves failed to open. An attempt was then made to initiate venting through the back up decay heat release system. When the decay heat relief control valve was opened, the valve discharge nozzle (4 1/2" OD) disengaged from the exhaust vent as a result of the initiating reaction force permitting the release of secondary steam to a small room of the turbine building.

b. RSS Action. This condition was considered as a contributor to the failure of the auxiliary feedwater system since the possibility of steam discharge into the room where the secondary safety/relief valves are located, could interact with the auxiliary feedwater system which could be needed to control plant heat removal following such high energy line breaks.

8. Consolidated Edison Co. (Indian Point) #65

a. Problem. Removal of the entire unirradiated core from the reactor vessel. The core consists of pressurized fuel rods which have experienced cladding collapse during long term irradiation. The collapse of the cladding has been attributed to densification of the pellets after prolonged service.

b. RSS Action. The impact of fuel densification as it concerns fuel cladding temperature margins during plant accidents and transients is covered in the AEC's licensing process and by the AEC's acceptance criteria for the design and performance of emergency core cooling systems. These analyses establish conservative thermal margins for full performance where densification is significant.

9. Georgia Power Co. (Hatch #1) #52

a. Problem. Flaws discovered at two recirculation inlet nozzles of the Reactor Pressure Vessel. On one nozzle a crack having an approximate dimension of 0.6 inches in the through-wall direction, located in the heat affected zone between the weld metal and vessel plate material.

b. RSS Action. This particular type of incident is accounted for predicting the probability of pressure vessel failure.

10. Commonwealth Edison Co. (Quad Cities 2) #56

a. Problem. Failure of four pipe hangers that support the 24" ring suction header located outside of the pressure suppression pool (Torus).

b. RSS Action. Failures of this type were examined to assess their contribution to pipe failure data. Failure of the header appeared as a potential failure mode of the vapor suppression system.

11. Commonwealth Edison Co. (Quad Cities 1) #58

a. Problem. The rapid closing of two circulating water system

reverse flow valves caused the rupture of an 8 foot diameter rubber expansion joint in the discharge line. As a result of the failure approximately 600,000 gallons of river water entered the turbine building. The flooding of the turbine building resulted in the loss of safety related equipment, i.e., cooling water pumps for two of the three station emergency diesel generators, all four service water pumps for unit 1 residual heat removal system and the station seismograph.

b. RSS Action. Pumps, valves and other equipment associated with Engineered Safety Systems have been examined as to their elevations and physical locations relative to important sources of water and included in fault trees where appropriate.

12. Northern States Power Co. (Monticello) #61

a. Problem. Loss of generator excitation caused a turbine trip and reactor scram. A group 1 isolation signal of undetermined cause was received, resulting in the closing of the main steam isolation valves. During the ensuing pressure transient the reactor reached a maximum pressure level of 1140 psig. Relief valves A, B, and C operated but relief valve "D" failed to operate. The "A" safety valve operated (1220 psig setpoint) and the thermocouple for the "D" safety valve showed a temperature increase indicating that it may have leaked a small amount of steam. A high drywell pressure alarm was also received. The Emergency Core Cooling systems, with the exception of the High Pressure Coolant Injection system (HPCI) which was isolated for surveillance testing started automatically.

b. RSS Action. Relief valve failures have been identified as a failure event on the automatic depressurization system (ADS) tree and failure of the HPCI system to operate due to isolation for surveillance testing has been identified on the HPCI fault tree.

13. Commonwealth Edison Co. (Quad Cities 2) #62

a. Problem. A fire in a cable tray resulted in the loss of "B" recirculation pump and erratic indication on some of the control room process instrumentation and damage to 24 electric cables. A controlled reactor shutdown was initiated.

b. RSS Action. The routing and separation of safety system cables in trays has been covered in the common mode failure analyses.

14. Commonwealth Edison Co. (Quad Cities 2) #64

a. Problem. The "B" recirculation pump tripped due to a problem in the speed control unit.

b. RSS Action. This type of transient is within the normal plant operating capability. However, this transient could result in a demand for reactor shutdown and is included in the data for initiating events for the transient event trees.

15. Commonwealth Edison Co. (Dresden 2) #66

a. Problem. In service inspection (Radiography) of "B" main steam piping showed the main steam flow restrictor to have failed at the weld securing the downstream cone. The loose cone lodged immediately upstream of the inboard MSIV.

b. RSS Action. This weld failure resulted in a loose part within the reactor coolant system. Loose parts that might interfere with the operability of systems and components, e.g., valves, were considered in the fault tree analyses.

16. Commonwealth Edison Co. (Dresden, 1, 2, and 3) #69

a. Problem. Failure of 40-50 feet of the dike for the 1275 acre cooling lake. Condenser cooling water supply was transferred to the Illinois river.

b. RSS Action. Loss of pump basin water has been identified as a failure event on the high pressure service water (HPSW) and

emergency service water (ESW) fault trees.

17. Millstone Point Company (Millstone 1) #70

a. Problem. Two of the four feedwater spargers contained circumferential cracks in the vicinity of their attachment welds. One sparger crack appeared to penetrate the full wall thickness and was, at least, one-half of the sparger circumference in length.

b. RSS Action. Cracks such as these could potentially lead to failure of the spargers. The sparger failure could lead to loss of the feedwater system. Failure of the feedwater system is included in the transient event trees. Operating data were used to estimate transient events with loss of feedwater.

18. Boston Edison Co. (Pilgrim 1) #71

a. Problem. After experiencing a flow biased flux scram the operator manually opened one relief valve to reduce system pressure, the valve failed to reseat. Approximately 10,000 gallons of water (primary) was discharged to the torus.

b. RSS Action. Operation of a relief valve and subsequent failure of the valve to close represent a small LOCA if the feedwater system fails to make-up the coolant inventory. The transient event tree analysis included stuck-open relief valves for both success and failure of the feedwater system to supply make-up inventory.

19. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #72

a. Problem. An increase in stack release rate was experienced while operating at 100% power (1593 MWT). Maximum release rate reached was 20,000 μCi/sec. Reactor power was reduced to 70% and release rate reduced to 18,000 μCi/sec.

b. RSS Action. This type of incident pertains to routine effluent releases and is not relevant to the RSS study of reactor accidents.

20. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #73

a. Problem. A fire occurred in the station unit auxiliary transformer following a turbine trip and subsequent motoring of the main generator. Cause of the fire was apparent failure of mal-operation of protective breakers for the generator and turbine.

b. RSS Action. Failure of major electric components that can result in failure of the electric power system to engineered safety features is identified on the fault trees and in common mode analyses.

21. Niagara Mohawk Power Corp. (Nine Mile Point 1) #75

a. Problem. Premature actuation of a safety valve resulted in release of primary steam to the containment drywell. A turbine trip also occurred.

b. RSS Action. Turbine trips or inadvertent safety valve actuations have been covered by the transient event tree analysis.

22. Vermont Yankee Nuclear Power Co. (Vermont Yankee) #76

a. Problem. Turbine gland seal failure while turbine was on the turning gear caused a small quantity of primary steam to leak from the turbine seals into the turbine building.

b. RSS Action. This type of failure could potentially result in a reactor shutdown which is accounted for in the transient event tree analysis.

23. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #77

a. Problem. Failure of a start up transformer caused the loss of station electric power and a resultant scram. During the ensuing primary system transient three of four relief valves actuated but one could not be verified to have opened due to a thermocouple malfunction.

b. RSS Action. See comment for item 14.

24. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #79

a. Problem. While calibrating the pump speed control system an increase in speed of one recirculation pump occurred. The ensuing transient resulted in a primary system pressure increase and an increase in the stack release rate from 0.05 Ci/Sec to 2.5 Ci/Sec.

b. RSS Action. See comment for item 19.

25. Millstone Point Co. (Millstone Point 1) #80

a. Problem. A manufacturing error to provide a specified chamber at the junction weld between the control rod blade sheath and the control rod blade limiter casting could result in a ledge that would interfere with fuel assemblies when the blade is within one inch of the fully inserted position.

b. RSS Action. This anomaly does not appear as a fault condition on the fault trees because insertion to one inch of full insertion is deemed adequate.

26. Jersey Central Power & Light Co. (Oyster Creek) #78

a. Problem. A malfunction relief valve caused a blowdown of the primary system following a reactor scram. During the ensuing transient one relief valve failed to reseat discharging 50,000 gallons of primary coolant to the torus.

b. RSS Action. See comment for item 18.

27. Millstone Point Co. (Millstone 1) #85

a. Problem. During inspection of the reactor internals, cracks were discovered in the NE and NW feedwater spargers. The maximum crack was estimated to be 4 inches long and 1/32 inches wide.

b. RSS Action. See comment for item 17.

28. Boston Eidson Co. (Pilgrim 1) #87

a. Problem. Strike against Boston Edison Co. by the Utility Workers of America (UWUA Local 387).

b. RSS Action. Not applicable to the considerations defined in the Reactor Safety Study.

29. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #89

a. Problem. Lightning struck the top of the ventilation stack disabling one of the two stack gas monitoring systems and the area gamma radiation monitor. The lightning also caused an explosion in the off-gas holdup system.

b. RSS Action. See comment for item 19.

30. Commonwealth Edison Co. (Quad Cities 2) #82

a. Problem. A lightning strike caused failure of a rupture disc in the off-gas holdup system.

b. RSS Action. See comment for item 19.

31. Commonwealth Edison Co. (Dresden 2) #83

a. Problem. Explosion in the off-gas system while making modifications.

b. RSS Action. See comment for item 19.

32. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #93

a. Problem. Lightning struck the ventilation stack disabling both stack gas monitors and the area gamma radiation monitor also causing an explosion in the off-gas holdup system.

b. RSS Action. See comment for item 19.

33. Iowa Electric Light & Power Co. (Duane Arnold) #92

a. Problem. Possibility that the fuel bundles have a manufacturing defect in the lower tie plate castings.

b. RSS Action. Defects of this type potentially involve considerations pertinent to flow blockage and emergency core cooling functionability. See Appendices I and V.

34. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #97

a. Problem. Inspection of fuel bundles revealed cracks in 5 of the fuel bundle channels.

b. RSS Action. See comment for item 33.

35. Millstone Point Co. (Millstone Point 1) #90

a. Problem. Assembly errors which led to the inverted installation of some control rod blades.

b. RSS Action. Analysis indicates that the fission process can be adequately controlled event with blades installed in this fashion.

36. Boston Edison Co. (Pilgrim 1) #94

a. Problem. Inadvertent opening of the "D" target relief valve and failure to reseat.

b. RSS Action. See comment for item 18.

37. Jersey Central Power and Light Co. (Oyster Creek) #95

a. Problem. During routine switching of electric loads to the startup transformer resulted in temporary loss of electrical power to essential equipment due to an improperly set tap on a differential current relay.

b. RSS Action. The fault tree for the electrical power system identifies faults which could cause an outage of power to safety system equipment including operator error for wrong set points.

38. Vermont Yankee Nuclear Power Corp. (Vermont Yankee) #100

a. Problem. During control rod friction drive tests on one control rod with the reactor vessel head removed, a scram occurred from high flux levels. Investigation revealed that an adjacent control rod was in the fully withdrawn position.

b. RSS Analysis. Events such as this one are not significant in the overall accident analysis.

39. Baltimore Gas and Electric Co. (Calvert Cliffs) #67

a. Problem. A concrete void in the area of the containment vertical tendon bearing plates on the inside rings was detected. One void has a depth of 12 inches encompassing a surface area of 15 square inches extending to the proximity of an adjoining bearing plate. In a second bearing plate a concrete void 6 inches deep over a surface area of 10 square inches with a crack at the bottom of the void.

b. RSS Action. Lack of concrete consolidation and voids were construction deficiencies identified during plant construction and prior to plant operation. This detection and control is indicative of implementation of a program of quality assurance during the construction phase. If this type of deficiency had remained undetected in contruction, it could have affected the strength of the containment barrier if the containment were subjected to high overpressures after a loss of coolant accident. Consideration was given to the possible existence of such containment deficiencies in the study's estimation of predictable containment failure pressures. See Appendix VIII.

40. Virginia Electric and Power Co. (Surry 1) #68

a. Problem. A bonnet gasket on a 14 inch main feedwater line check valve failed releasing approximately 1000 gallons of secondary system water into the containment building.

b. RSS Action. Data on gasket failure and valve external leakage are a part of the data base where calculations have been performed to predict failure rates.

41. Yankee Atomic Electric Co. (Yankee) #74

a. Problem. Indications of binding during operations of the cruciform control rods prompted visual inspections which revealed two control rods had been displaced and that tie down bolts for the shrouds had separated and were located on the vessel lower core support plate.

b. RSS Action. See comments under item 6 regarding control rod binding and under item 3 regarding loose parts.

42. Southern California Edison Co. (San Onofre 1) #81

a. Problem. An earthquake with a magnitude of 5.2 on the Richter scale was detected by seismic detectors. No damage was reported.

b. RSS Action. The Design Adequacy portion of the Reactor Safety Study checked the capability of a plant to carry the design stresses produced by an earthquake. See Appendix X.

43. Florida Power and Light Co. (Turkey Point 3) #84

a. Problem. Loss of power from an Exide inverter while instrumentation was in a 1 out of 2 scram logic condition causing reactor shutdown and loss of offsite power.

b. RSS Action. Analysis of this type of incident is covered in the electrical power system fault trees because the failure causes reactor shutdown. Turbine trip has been evaluated for its contribution to loss of offsite power to the plant. Its contribution to transient initiating events is covered by the transient event tree.

44. Southern California Edison Co. (San Onofre 1) #88

a. Problem. While the reactor was shut down and maintenance was being performed on one of the offsite electrical sources for the plant, the alternate offsite electrical feed to the plant was interrupted by the inadvertent actuation of a differential current protection relay. This resulted to a loss of all offsite power into the plant, and the contributing fault was attributed to improper grounding of protection systems for the main station generator. The emergency onsite power source (provided by two diesel generators) started and operated the necessary plant heat removal equipment. After about 3/4 of an hour operation, a malfunction in voltage regulator for one diesel generator resulted in an overload trip of both the emergency onsite power sources. A momentary (about 1 minute) interruption of the emergency power source occurred as a result of this common fault.

b. RSS Action. Considerations (through fault trees, event trees and data application) were given to such types of faults that could result in an interruption and loss of both the offsite and onsite sources of electrical power for the plant. Assessment of the probability and consequences from such an event as loss of all electric power to a plant was an important part of this study effort.

45. Consumers Power Company (Palisades) #98 and ROE 74-3

a. Problem. Mechanical Vibrations of Reactor Internals. Inspection revealed the following:

1. All expansion-compensating ring bolts were found broken.

2. Measurements in the proximity of the upper guide structure reveal that the core support barrel is nominally 1/4" lower than as-built drawings specify.

3. The core support barrel flange has worn a ledge in the vessel flange permitting the core support barrel flange to be vertically displaced.

4. A groove approximately 1/16" deep and 1/4" wide was worn into the reactor vessel head flange when the

compensating ring made contact with the vessel head.

b. RSS Action. Analysis indicates this relates to ECCS functionability questions which are covered in Appendix V.

46. Florida Power and Light Co. (Turkey Point 3 & 4) #99

a. Problem. Utility workers on strike with threats of sabotage of a main generator at the plant.

b. RSS Action. Potential accidents due to sabotage have not been an explicit part of the Reactor Safety Study.

47. Consumers Power Co. (Milford 1 & 2) #101

a. Problem. Deficiencies in Cadweld splicing of concrete reinforcing bars.

b. RSS Action. See comment for item 39.

48. Consolidated Edison Co. (Indian Point 2) #102

a. Problem. A crack in the 18 inch feedwater line to steam generator #2 resulted in the discharge of water and steam to the containment vessel. The crack was not isolatable from the steam generator. The crack is located several inches inside the containment vessel, is circumferential, extends approximately one half the circumference of the pipe, and appears to be associated with a fillet weld, joining the end plate of the containment penetration bellows assembly to the feedwater line.

b. RSS Action. Pipe ruptures for all systems show on individual system fault trees. Pipe leaks and ruptures are also covered by the data base.

49. Virginia Electric Power Co. (Surry 1) #103

a. Problem. Loss of flow in the "A" main coolant loop due to a broken pump shaft in Reactor Coolant Pump (RCP) "A". The break was 15 inches above the impeller, between the thermal barrier and the lower pump bearing.

b. RSS Action. This event resulted in a loss of flow in one RCS loop. Such transients are accounted for in the plant design. Potential shutdowns of the reactor are covered by the transient event tree.

50. Duke Power Co. (Oconee 2) #106

a. Problem. The failure of a reactor coolant pump seal caused leakage of primary water to the floor of the containment building.

b. RSS Action. Leakage due to the failure of a coolant pump seal is within the capability of normal RCS inventory make-up systems. The event trees consider small LOCA conditions more severe than this event.

Reference

1. Williams, H.L., "Reliability Evaluation of the Human Component in Man-Machine Systems", Electrical Manufacturing, 1958, 4, 78-82.

TABLE III 3-1 NUMBER OF FAILURES BY PLANT SHOWING FAILURES DURING STANDBY AND OPERATIONS

1972 DATA

Reactor	Plant Type	Standby	Oper.	Months Oper. Time	Hours Oper. Time	% Standby	% Oper.
Dresden 1	BWR	1	2	12	8760	33.4	66.6
Yankee	PWR	8	5	12	8760	61.5	38.5
Indian Point 1	PWR	7	12	12	8760	36.8	63.2
Humboldt Bay 3	BWR	5	7	12	8760	41.7	58.3
Big Rock Point	BWR	4	3	12	8760	57.1	42.9
San Onofre 1	PWR	3	7	12	8760	30.0	70.0
Haddam Neck	PWR	0	3	12	8760	----	100.0
Nine Mile Point 1	BWR	7	13	12	8760	35.0	65.0
Oyster Creek	BWR	10	19	12	8760	34.5	65.5
Ginna	PWR	1	5	12	8760	16.7	83.3
Dresden 2	BWR	8	20	12	8760	28.6	71.4
Point Beach 1	PWR	2	4	12	8760	33.3	66.7
Millstone 1	BWR	7	22	12	8760	24.1	75.9
Robinson 2	PWR	3	17	12	8760	15.0	85.0
Monticello	BWR	10	34	12	8760	22.7	77.3
Dresden 3	BWR	4	22	12	8760	15.4	84.6
Palisades	PWR	6	22	12	8760	21.4	78.6
		86	217	204	148,920	XXXX	XXXX

TABLE III 3-2 NUMBER OF FAILURES BY PLANT COMPONENT/SYSTEM

Reactor	Battery	Condenser	Control Rods	Containment	Diesel	Gen. Elect.	Electrical Breaker	Elect. Switch	Gen. Steam	Instruments	Human Error	Pipe	Power Emerg.	Power Off-Site	Transformer	Turbine	Valves	Pumps	Miscellaneous	TOTAL
Dresden 1												1					2			3
Yankee Rowe	1		5		3	1				1							2			13
Indian Point 1			2						2	0	2	1		2		1	8	1		19
Humboldt Bay 3				1	2		1	1		1				3			3			12
Big Rock Point					2					2				1			2			7
San Onofre 1			1			2			2								3	1	1	10
Connecticut Yankee																	3			3
Nine Mile Point 1								2		1	1	1					8	4	3	20
Oyster Creek	1		1		2					5	4	3				1	6	3	3	29
Ginna							1			1	1	1							2	6
Dresden 2					3					11							10	4		28
Point Beach 1							1		1		2	1							1	6
Millstone 1					1					12		2	2	1			3	1	6	29
Robinson 2			2		3		1		1	1							7	1	4	20
Monticello			5		2			1	1	5	1						21	6	2	44
Dresden 3										7		1				1	15		2	26
Palisades			7		3					1	3				1		9	3	1	28
TOTALS	2	0	23	1	21	3	4	4	7	48	14	11	2	7	1	3	102	24	26	303

TABLE III 3-3 AVERAGED FAILURE RATE ESTIMATES
(Rounded to nearest half exponent)

Component	PWR				BWR				COMBINED			
	T	N_pN_c	n_f	λs/hr	T	N_pN_c	n_f	λs/hr	T	N_pN_c	n_f	λs/hr
Pumps	8760	400	6	1×10^{-6}	8760	450	18	3×10^{-6}	8760	850	24	3×10^{-6}
Piping[a]	8760	280k	3	1×10^{-9}	8760	315k	8	3×10^{-9}	8760	595k	11	1×10^{-9}
Control rods[b]	8760	400	4	1×10^{-6}	8760	1350	2	1×10^{-7}	8760	1700	6	3×10^{-7}
Diesels	8760	24	9	3×10^{-5}	8760	27	12	3×10^{-5}	8760	51	21	3×10^{-5}
Valves	8760	2312	32	1×10^{-6}	8760	1467	70	3×10^{-6}	8760	3842	102	3×10^{-6}
Instruments	8760	2560	6	3×10^{-7}	8760	3042	44	1×10^{-6}	8760	5613	50	1×10^{-6}

(a) Failure rate given in units of per hour per foot, where 280k denotes approximately 280,000 ft.

(b) Failure rate per hour per rod, for failure to enter.

TABLE III 3-4 AVERAGED DEMAND PROBABILITY ESTIMATES
(Rounded to nearest half exponent)

Component	PWR				BWR				COMBINED			
	n_f	N_pN_c	N_T	Q_d	n_f	N_pN_c	N_T	Q_d	n_f	N_pN_c	N_T	Q_d
Pumps	6	400	12	1×10^{-3}	18	450	12	3×10^{-3}	24	850	12	1×10^{-3}
Control Rods	4	400	12	1×10^{-3}	2	1350	12	1×10^{-4}	6	1700	12	3×10^{-4}
Diesels	9	24	12	3×10^{-2}	12	27	12	3×10^{-2}	21	51	12	3×10^{-2}
Valves	32	2312	12	1×10^{-3}	70	1467	12	3×10^{-3}	102	3842	12	1×10^{-3}
Instruments[a]	6	2560	1.5	1×10^{-3}	44	3042	1.5	1×10^{-2}	50	5610	1.5	3×10^{-3}

(a) Average number of instrumentation tests obtained from histogram of test distributions for safeguard instrumentation.

TABLE III 3-5 1972 FAILURE CATEGORIZATION INTO RANDOM VERSUS COMMON MODE

Reactor	PWR				BWR			
	Random		Common Mode		Random		Common Mode	
	Number	Percent	Number	Percent	Number	Percent	Number	Percent
Dresden 1					3	100.0		
Yankee Row	12	92.3	1	7.7				
Indian Point 1	19	100.0						
Humboldt Bay 3					10	83.3	2	16.7
Big Rock Point					5	71.4	2	28.6
San Onofre 1	9	90.0	1	10.0				
Haddam Neck	3	100.0						
Nine Mile Point 1					17	85.0	3	15.0
Oyster Creek					27	93.1	2	6.9
Ginna	4	66.7	2	33.3				
Dresden 2					24	85.7	4	14.3
Point Beach 1	4	66.7	2	33.3				
Millstone 1					28	96.6	1	3.4
Robinson 2	18	90.0	2	10.0				
Monticello					37	84.1	7	15.9
Dresden 3					25	96.2	1	3.8
Palisades	25	89.3	3	10.7	—		—	
TOTAL	94		11		176		22	

TABLE III 3-6 COMMON MODE EFFECTS AND CAUSES

	PWR (percent)	BWR (percent)
A. Component Effect	9.1	22.7
B. System Effect	18.1	4.5
C. Interaction Effect	9.1	4.5
1. Design, etc. Cause	27.3	13.6
2. Human Cause	18.2	18.3
3. Environment Cause	9.1	13.6
4. Hardware Cause	----	6.3

(OTHERS QUESTIONABLE)

Section 4
Expanded Final Data Assessment

4.1 INTRODUCTION

Tables III 4-1 and III 4-2 in this section present as a separate tabulation the final assessed data base utilized in the study. The information is extracted from the tables in section 2 and includes further elaboration on applicability considerations for safeguard related components. Except for pumps, the applicable environment for these tables consists of standard operational nuclear power plant conditions (as characterized in the model descriptions). The assessed ranges cover variations which can occur in these environments. Pump failure to run, given successful start, was also assessed for extreme temperature and pressure conditions characterizing a severe accident. Table III 4-3 gives additional data assessments for post-accident conditions for certain other components relevant to the study. A discussion is provided for a component when further relevant details are applicable.

The tables contain the assessed ranges for the data, the median value of the range and the error factor. The range represents a 90% probability, or ("confidence level"), associated with the random variable approach. The median is a reference value for the range; there is a 50-50 chance that the data value is either higher or lower than the median value. The error factor is the upper limit of the range divided by the median value. Since the median is the geometric midpoint, the error factor is also the median divided by the lower limit. The values given in the tables are rounded to the nearest half exponent value (i.e., 1 or 3 appearing as the significant figure). Units for the data are probability per demand, "d", or per hour, "hr".

4.1.1 NOTES ON PUMPS

a. Test and Maintenance.

Generally, those test and maintenance situations where an override feature can automatically return the pump (or other devices) to operational status, given demand will have no test and maintenance contribution to unavailability. Distributions on test and maintenance act durations are used to account for variations in the times required to complete the act from plant to plant or situation to situation. Testing times include the time required to make the minor repairs incidental to the tests.

Testing the pumps within the safety systems requires isolation of the pump under test in the majority of cases. This results in a contribution to unavailability due to pump downtime. In general, the probabilistic contribution is derived from the test act duration time which ranges (90%) from 15 minutes to 4 hours, under a log-normal distribution.[1] From this range, the mean test duration time (downtime) is thus 1.4 hours (t_D = 1.4 hours for test).

Maintenance on the pumps ranges in duration from 30 minutes to several days. From this range the mean maintenance act duration t_D is 37 hours. Maximum outage during powered operation may be limited to 24 hours on pumps other than those located inside containment. Use of the 24 hour limit as an upper bound gives a mean maintenance act duration, (t_D), of 7 hours. Pumps located inside the containment vessel are permitted by specification to be down singly for a maximum of 72 hours during plant operation. The associated mean duration time for these particular pumps is t_D = 19 hours.

In general, the test period for safety system pumps is fixed by the specification at monthly intervals. The test frequency is therefore approximately constant at 1 act per month. The nominal test contribution to unavailability, Q_T, is the ratio of mean test act duration time (t_D), to test interval.

$$Q_T = \frac{t_D}{\#Hrs/Month}$$

[1] See section on test and maintenance data.

Non-routine maintenance ranges from monthly to yearly with a mean pump maintenance interval of 4.5 months/act or a mean frequency of maintenance of 0.22 acts/month. The maintenance contribution to unavailability Q_M is a function of the maintenance frequency (f), mean maintenance act duration (t_D), and maintenance interval. The equation for Q_M is given by the equation

$$Q_M = f \times \frac{t_D}{720},$$

when t_D is now the average maintenance downtime. Substituting values into the above equations will give numerical values for Q_M.

b. Environments.

The safety pumps located outside containment are not likely to be subjected to abnormal environmental conditions in the event of the assumed loss of coolant accident with the exception of a temporary change in temperature and radiation level of the pumped fluid. Since these pumps are designed for such conditions, the assessments for outside pumps are based on performance data from similar pumps operating under design conditions.

The pumps located inside containment may be subjected to a much more severe environment during the period from the accident to the time that the safety system can reduce the temperature, pressure, humidity, and radiation levels to near normal. This extreme environmental condition has a chance of subsiding within 24 hours.

The levels of the immediate post-accident environment cannot be determined exactly, but conditions generally representative of the accident were used in a series of pump qualification tests for the inside pumps. These tests were non-exhaustive. The results of these tests and experience data from pump performance in test reactors operating at extremely high temperatures were considered in making the assessments for pumps inside containment. Recovery to near normal environmental conditions is likely to increase the probability of continued pump operation. Experience and testing (Ref. 1, 2, 3, 4) have revealed, however, some degradation in lubricants, bearings, and motor insulation after exposure, possibly degrading pump performance given survival of the initial 24-hour period. To account for the potential degradation, a failure probability between normal and abnormal conditions is assigned with sufficient associated uncertainties to account for the possibility of deviations.

4.1.2 NOTES ON VALVES

a. Failure Modes.

Failure of a valve to operate includes changing state from closed to open or open to closed. Failure to remain open (plug) refers to reduction of flow to an unusable level due to foreign material or gate failure, etc. Not included in the data is the contribution for an inadvertent or false signal driving valves closed. Instances of valve gates separating from drive stems and lodging in a closed position (while the valve monitors continued to indicate open) have been reported in nuclear operating experience.

b. Test and Maintenance.

Motor operated valve test act duration times range from 15 minutes to 2 hours (90% range) with a mean test time t_D of 0.86 hours (log-normal). No downtime test contribution is obtained if the valve has a test override feature which automatically returns the valve to an operational status given demand. The position monitors used on automatic valves detect the position of valve drive; they do not determine flow or position of valve gate. Hence monitoring does not influence fault duration time for failure to remain open (plug) failure modes.

Valve outages for maintenance range from 30 minutes to several days with a mean maintenance duration t_D of 24 hours. Maintenance acts on certain valves may be limited to 24 hours during powered operations by specification. Under these conditions the mean act duration time t_D is 7 hours. The mean maintenance act frequency f is 0.22 acts per month. Thus,

$$Q_T = \frac{t_D}{720}, \quad Q_M = \frac{ft_D}{720},$$

where t_D in the first equation is the test downtime and in the second

equation maintenance downtime. Substituting will yield the applicable numerical values for Q_T and Q_M.

c. Environments.

In general, valves within the safety system operate on demand within a few minutes after the accident. Hence degradation due to post-accident environments is deemed not significant within the associated uncertainties.

4.1.3 NOTES ON PIPE - TESTING

Certain safety piping is tested monthly during the tests on pumps within the safety system. Certain portions of the piping however are incapable of being periodically tested except during the initial tests prior to final licensing of the plant.

Therefore the failure rate assessments were applied to both standby pipes (safety) and active pipes (process) with large uncertainties to account for the possibility of either extreme. The safety assessments are given in units of per section per hour with a section defined as an average length between major discontinuities such as valves, pumps, etc. (approximately 10 to 100 feet). Each section can include several welds, elbows and flanges. See special assessment section of this appendix for more details.

4.1.4 NOTES ON MOTORS

In many instances, pumps and valves within the safety system are driven by electric motors. Available experience data do not permit separation of motor failure from pump failure. Therefore, separate motor failure rates for pump and valve drive motors should not be included. The assessments above apply to those electric motors that function independently of the pump and valves.

4.1.5 NOTES ON RELAYS - FAILURE MODES

The available data do not completely isolate separate causes of failure; hence the above failure modes are not necessarily independent. For example, failure rates for failure to energize includes failure of the normally open contacts to close. Hence relay and contact failure rates in general should not be combined together to determine overall relay failure rates. Individual contributions, however, can be employed where there are individual, separate effects on the system. Examples are failure of contact of a multiple contact relay, or shorts to power (which could effect power circuit) if these modes have a unique, individual effect on the system.

4.1.6 NOTES ON SWITCHES - FAILURE MODES

The data do not uniquely separate the causes of failure; hence the above failure modes are not necessarily independent. Failure to operate includes failure of contacts. In general, the contact contribution should not be added to the switch contribution to determine overall switch failure rate. As with relays, when separate, individual effects occur, individual contact contributions can be computed (such as for multiple contact switches).

4.1.7 NOTES ON BATTERIES - FAILURE MODES

The emergency dc power system involves 58-60 series connected lead cadmium or lead calcium battery cells to form a 125 volt supply. Two 125 volt systems are series connected to obtain 250 volts. These batteries are constantly charged by chargers and the open circuit output voltage monitored at regular intervals. The significant failure mode in this arrangement involves failure to provide adequate output voltage under emergency load conditions. Failures by shorts to ground or internal shorts within cells are likely to be detected quickly with negligible resulting fault duration time.

4.1.8 NOTES ON SOLID STATE DEVICES

a. Environments. High power application is defined as application in circuits involving currents of 1 ampere or above and/or voltages - 28 volts and above.

b. Failure Modes. The available data do not permit separation of the causes of failure in all cases; hence the above failure modes are not independent. Failure rates for shorts should not be added to rates for failure to function unless special consideration of short failures is necessary due to unique effects on the system.

The relatively large error factors on solid state device assessments reflect the potential variation from application to application. For particular situations, a detailed analysis could yield narrower bounds.

4.1.9 NOTES ON DIESELS

a. Test and Maintenance. Certain specific tests on emergency diesel generators render the power plant unavailable for use in the event of a demand on the equipment. The duration of these tests ranges from 15 minutes to 4 hours with a mean test act duration time t_D, of 1.4 hours.

Maintenance acts on diesels range in duration from 2 hours to 160 hours. The mean maintenance act duration is 21 hours. If specifications limit the maximum diesel outage during plant operation to 24 hours the associated mean is then 13 hours.

b. Failure Modes. The demand probabilities on failure to start involves the complete plant including starters, pumps and fueling systems. Because of possible variance in the redundancy of auxiliary equipment, the operational failure rate for the engine is separated from the operational failure rate for the complete power generator system.

c. Environments. These above data apply to diesel operation in normal environments. Diesels operating in extreme weather conditions or with exhaust outlets near the intake air vents, etc., may have significantly higher operational failure rates due to the sensitivity of the system to intake air quality. These should be assessed on an individual basis.

4.1.10 NOTES ON INSTRUMENTATION - FAILURE MODES

The data for shift in calibration incorporate a variation of drift magnitude. These data may be pessimistic if used for instrumentation with wide operational tolerance bands. In these cases individual assessment should be performed.

The relatively large error factors associated with instrumentation assessments reflect the wide variation in configuration from application to application. For any particular instrumentation system, a detailed analysis may be done to obtain narrower bounds.

4.1.11 NOTES ON WIRES AND TERMINAL BOARDS - FAILURE MODES

The failure rates for wires are based on a typical control circuit wire section with soldered and lug connections to components and terminal boards. The circuit consists of approximately 30 connections with approximately 20 of these connections comprised of lug terminals on terminal boards.

The data do not permit a unique separation of failure modes in all cases; hence the failure modes listed for wires and terminals are not necessarily independent. Probabilities for defective terminations should not in general be added to wire probabilities to obtain overall circuit probabilities. Separate terminal board data are provided for those cases in which unique system effects exist.

4.2 SUMMARY OF POST ACCIDENT ASSESSMENTS

Table III 4-3 summarizes the assessments pertaining to leak failures of the containment system, and the associated hardware in the post-accident situation. At the time of a severe loss-of-coolant accident the pressure within the containment system may rise to 40-45 psig from normal operating pressures. This pressure rise is expected to be rapid, but should subside in a few minutes if the safety system performs as intended. In the event of safety system failure, the conditions may exceed the design limits of the system. Those assessments derived from data from hardware operating within design limits apply only to conditions given safeguard system operation.

4.2.1 NOTES ON CONTAINMENT HARDWARE - TEST

Normally the containment system is at or slightly below atmospheric pressure with continuous monitoring of the internal containment environment; hence significant leaks occurring prior to an accident should be quickly detected. The capability of the system to withstand high pressure is verified at three year intervals by pressurizing the system to the design levels.

4.2.2 GENERAL DATA BEHAVIOR

The assessments used in the study are grouped and plotted in the following figures to show trend and class behavior. In the assessment process, these types of plots were also used to help check the overall consistency of the final data base.

Figure III 4-1 is a summary of the relative failure assessments for seven

classes of switching components.[1] The assessments are plotted as demand failure probabilities, and are shown in descending order of magnitude.

Figure III 4-2 is a summary of the relative failure assessments for five classes of valves. The assessments are plotted as demand failure probabilities, and are shown in descending order of magnitude.

Figure III 4-3 is a summary of the assessments for the operational failure rate of pumps, given proper start for three different environmental levels. The plots are in operational failure rates per hour and are shown in decreasing severity of the environment.

Figure III 4-4 is a summary of the demand failure probabilities for four general classes of hardware. Class 1 contains heavy mechanical equipment such as diesel generators; Class 2 electromechanical devices such as motors, clutches, etc.; Class 3 includes mechanical devices such as pumps and valves; and Class 4 electrical equipment such as circuit breakers, relays, etc.

Figure III 4-5 is a summary of the gross leak and rupture assessments for the passive safeguard and containment associated hardware.

---

[1]The figures are at the end of the text.

References

1. WCAP-7744, "Environmental Safety Features Related Equipment, Volumes 1 and 2 (NSSS Standard and Nonstandard Scope)," December 1971, J. Locante, E. G. Igne. Non-Proprietary Class 3.

2. WCAP-7829, "Fan Cooler Motor Unit Test," April 1972, C. V. Fields. Non-Proprietary Class 3.

3. WCAP-7343-L, "Topical Report - Reactor Containment Fan Cooler Motor Insulation Irradiation Testing", July 1969, J. Locante (Westinghouse NES Proprietary Class 2).

4. WCAP-7396-L, "Safety Related Research and Development for Westinghouse Pressurized Water Reactors - A Program Outline, Spring 1969," April 1969, R. M. Hunt (editor). (Westinghouse NES Proprietary Class 2)

TABLE III 4-1 SUMMARY OF ASSESSMENTS FOR MECHANICAL HARDWARE

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Pumps (includes driver)	Failure to start on Demand, Q_d [a]	3×10^{-4} - 3×10^{-3}/d	1×10^{-3}/d	3
	Failure to run, given start, λ_o (normal environments):	3×10^{-6} - 3×10^{-4}/hr	3×10^{-5}/hr	10
	Failure to run, given start, λ_o (extreme, post accident environments inside containment):	1×10^{-4} - 1×10^{-2}/hr	1×10^{-3}/hr	10
	Failure to run, given start, λ_o (post accident, after environmental recovery).	3×10^{-5} - 3×10^{-3}/hr	3×10^{-4}/hr	10
Valves				
Motor Operated:	Failure to operate, Q_d (includes driver) [b]:	3×10^{-4} - 3×10^{-3}/d	1×10^{-3}/d	3
	Failure to remain open, Q_d (plug) [c].	3×10^{-5} - 3×10^{-4}/d	1×10^{-4}/d	3
	λ_s.	1×10^{-7} - 1×10^{-6}/hr	3×10^{-7}/hr	3
	Rupture, λ_s.	1×10^{-9} - 1×10^{-7}/hr	1×10^{-8}/hr	10

TABLE III 4-1 (Continued)

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Solenoid Operated:	Failure to operate, $Q_d^{(d)}$:	$3x10^{-4}$ - $3x10^{-3}$/d	$1x10^{-3}$/d	3
	Failure to remain open, Q_d(plug):	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Rupture, λ_s:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Air-Fluid Operated:	Failure to operate, $Q_d^{(a)}$:	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Failure to remain open, Q_d (plug):	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	λ_s:	$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Rupture, λ_s:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Check Valves:	Failure to open, Q_d:	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Internal leak, λ_o (severe):	$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Rupture, λ_s:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Vacuum Valve:	Failure to operate, Q_d:	$1x10^{-5}$ - $1x10^{-4}$/d	$3x10^{-5}$/d	3
Manual Valve:	Failure to remain open, Q_d (plug):	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Rupture, λ_s:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Relief Valves:	Failure to open, Q_d:	$3x10^{-6}$ - $3x10^{-5}$/d	$1x10^{-5}$/d	3
	Premature open, λ_o:	$3x10^{-6}$ - $3x10^{-5}$/hr	$1x10^{-5}$/hr	3

TABLE III 4-1 (Continued)

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Test Valves, Flow Meters, Orifices:	Failure to remain open, Q_d (plug).	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Rupture, λ_s:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Pipes Pipe ≤ 3" dia per section	Rupture/Plug, λ_s, λ_o:	$3x10^{-11}$ - $3x10^{-3}$/hr	$1x10^{-9}$/hr	30
Pipe > 3" dia per section.	Rupture/Plug, λ_s, λ_c:	$3x10^{-12}$ - $3x10^{-9}$/hr	$1x10^{-10}$/hr	30
Clutch, mechanical:	Failure to operate, Q_d (d)	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
Scram Rods (Single):	Failure to insert·	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3

(a) Demand probabilities are based on the presence of proper input control signals. For turbine driven pumps the effect of failures of valves, sensors and other auxiliary hardware may result in significantly higher overall failure rates for turbine driven pump systems.

(b) Demand probabilities are based on presence of proper input control signals.

(c) Plug probabilities are given in demand probability, and per hour rates, since phenomena are generally time dependent, but plugged condition may only be detected upon a demand of the system

(d) Demand probabilities are based on presence of proper input control signals.

TABLE III 4-2 SUMMARY OF ASSESSMENTS FOR ELECTRICAL EQUIPMENT

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Clutch, Electrical:	Failure to operate, Q_d (a):	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Premature disengagement, λ_o:	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
Motors, Electric:	Failure to start, Q_d (a):	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Failure to run, given start, λ_o (normal environment):	$3x10^{-6}$ - $3x10^{-5}$/hr	$1x10^{-5}$/hr	3
	Failure to run, given start, λ_o (extreme environment):	$1x10^{-4}$ - $1x10^{-2}$/hr	$1x10^{-3}$/hr	10
Relays:	Failure to energize, Q_d (a):	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Failure of NO contacts to close, given energized, λ_o:	$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Failure of NC contacts by Opening, given not energized, λ_o:	$3x10^{-8}$ - $3x10^{-7}$/hr	$1x10^{-7}$/hr	3
	Short across NO/NC contact, λ_o:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
	Coil open, λ_o:	$1x10^{-8}$ - $1x10^{-6}$	$1x10^{-7}$/hr	10
	Coil Short to power, λ_o:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10

TABLE III 4-2 (Continued)

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Circuit Breakers:	Failure to transfer, Q_d [(a)]:	$3x10^{-4}$ - $3x10^{-3}$/d	$1x10^{-3}$/d	3
	Premature transfer, λ_o:	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
Switches				
Limit:	Failure to operate, Q_d:	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
Torque:	Failure to operate, Q_d:	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
Pressure:	Failure to operate, Q_d:	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
Manual:	Failure to transfer, Q_d:	$3x10^{-6}$ - $3x10^{-5}$/d	$1x10^{-5}$/d	3
Switch Contacts:	Failure of NO contacts to close given switch operation, λ_o:	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
	Failure of NC by opening, given no switch operation, λ_o:	$3x10^{-9}$ - $3x10^{-7}$/hr	$3x10^{-8}$/hr	10
	Short across NO/NC contact, λ_o:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Battery Power Systems (wet cell):	Failure to provide proper output, λ_s:	$1x10^{-6}$ - $1x10^{-5}$/hr	$3x10^{-6}$/hr	3

TABLE III 4-2 (Continued)

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Transformers:	Open Circuit primary or secondary, λ_o:	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
	Short primary to secondary, λ_o:	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
Solid State Devices, Hi power Applications (diodes, transistors, etc.):	Fails to function, λ_o:	$3x10^{-7}$ - $3x10^{-5}$/hr	$3x10^{-6}$/hr	10
	Fails shorted, λ_o:	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
Solid State Devices, Low power Applications:	Fails to function, λ_o:	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
	Fails shorted:	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
Diesels (Complete plant):	Failure to start, Q_d:	$1x10^{-2}$ - $1x10^{-1}$/d	$3x10^{-2}$/d	3
	Failure to run, emergency conditions, given start, λ_o:	$3x10^{-4}$ - $3x10^{-2}$/hr	$3x10^{-3}$/hr	10
Diesels (Engine only):	Failure to run, emergency conditions, given start, λ_o:	$3x10^{-5}$ - $3x10^{-3}$/hr	$3x10^{-4}$/hr	10

TABLE III 4-2 (Continued)

Components	Failure Mode	Assessed Range	Computational Median	Error Factor
Instrumentation - General (Includes transmitter, amplifier and output device):	Failure to operate, λ_o:	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
	Shift in calibration, λ_o:	$3x10^{-6}$ - $3x10^{-4}$/hr	$3x10^{-5}$/hr	10
Fuses:	Failure to open, Q_d:	$3x10^{-6}$ - $3x10^{-5}$/d	$1x10^{-5}$/d	3
	Premature open, λ_o:	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
Wires (Typical circuits, several joints):	Open circuit, λ_o:	$1x10^{-6}$ - $1x10^{-5}$	$3x10^{-6}$/hr	3
	Short to ground, λ_o:	$3x10^{-8}$ - $3x10^{-6}$/hr	$3x10^{-7}$/hr	10
	Short to power, λ_o:	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Terminal Boards:	Open connection, λ_o:	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
	Short to adjacent circuit, λ_o:	$1x10^{-9}$ - $1x10^{-7}$	$1x10^{-8}$/hr	10

(a) Demand probabilities are based on presence of proper input control signals.

TABLE III 4-3 SUMMARY OF POST ACCIDENT ASSESSMENTS

Component	Failure Mode[a]	Assessed Range	Computational Median	Error Factor
Welds (containment quality):	Leak, λ_o (post accident, serious):	$1x10^{-10}$ - $1x10^{-7}$/hr	$3x10^{-9}$/hr	30
Elbows, Flanges, Expansion joints (containment quality):	Leak, λ_o (post accident, serious):	$1x10^{-8}$ - $1x10^{-5}$/hr	$3x10^{-7}$/hr	30
Gaskets (containment quality):	Leak, λ_o (post accident, serious):	$1x10^{-7}$ - $1x10^{-4}$/hr	$3x10^{-6}$/hr	30

(a) For assessments of containment system rupture probabilities, see the special assessment section of this appendix.

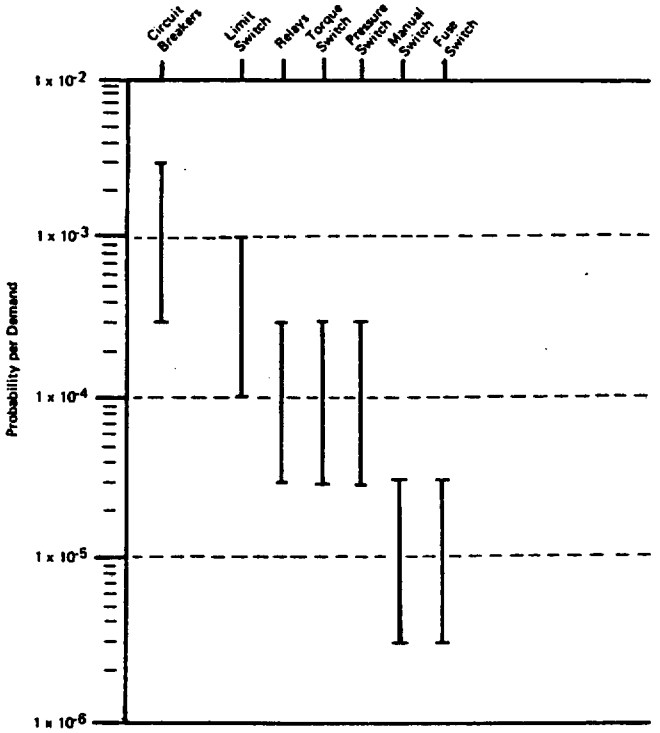


FIGURE III 4-1 Relative Failure Rate Assessments - Switches

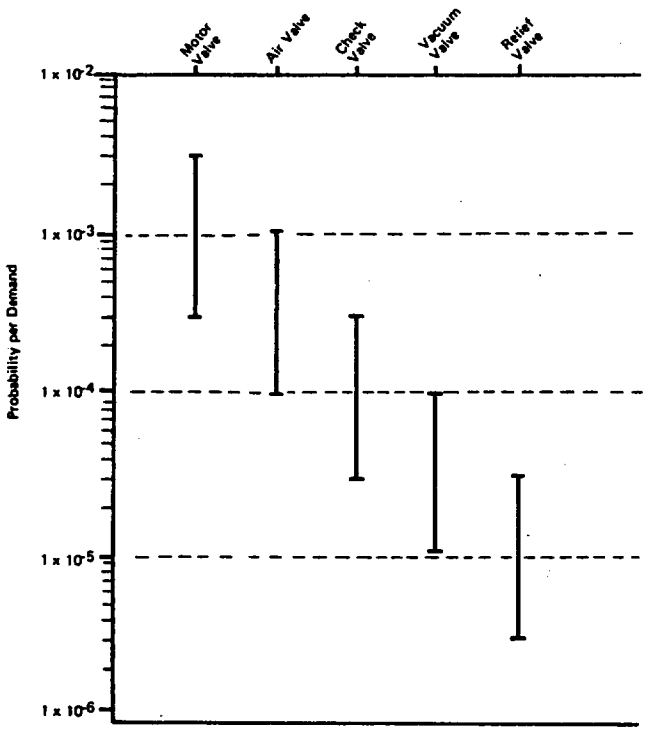


FIGURE III 4-2 Relative Failure Rate Assessments - Valves

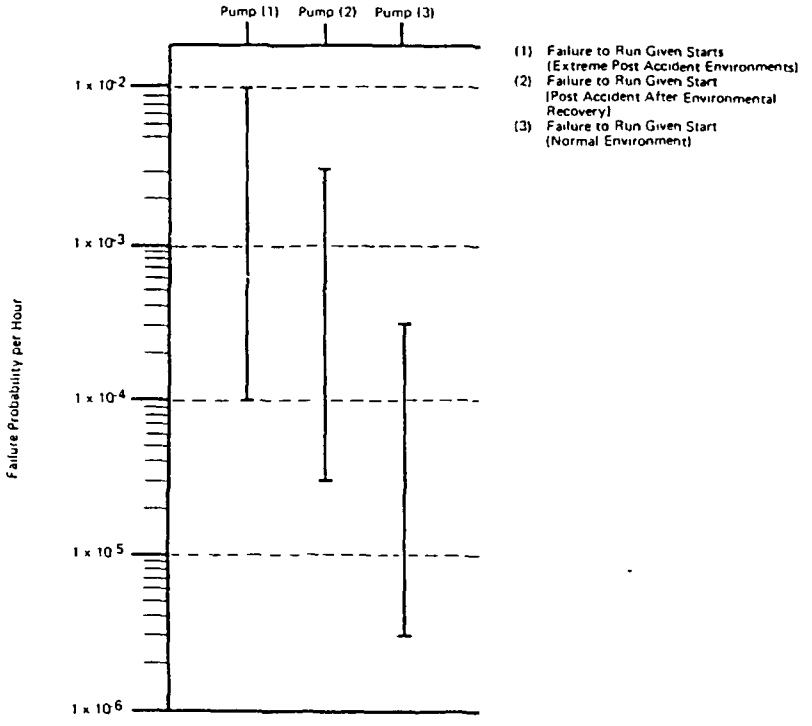


FIGURE III 4-3 Relative Failure Rate Assessments - Pumps

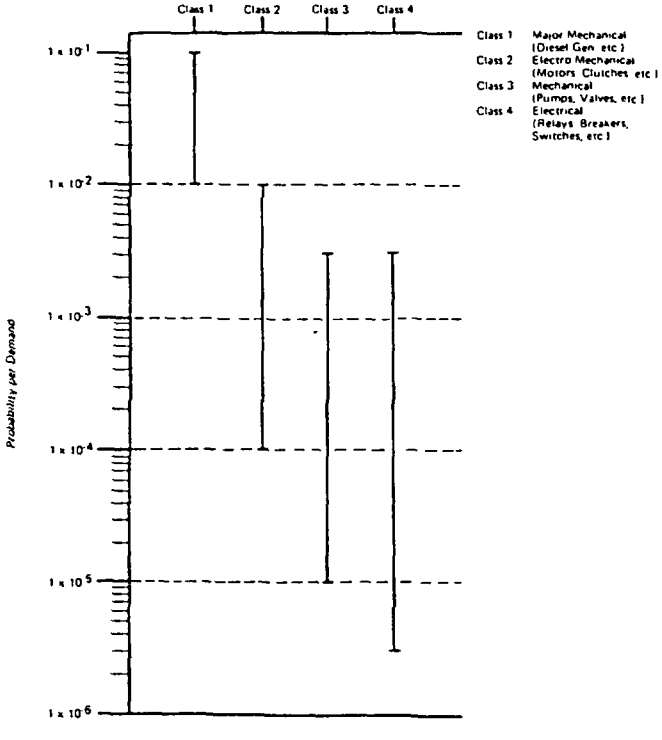


FIGURE III 4-4 Demand Probabilities of Classes of Hardware

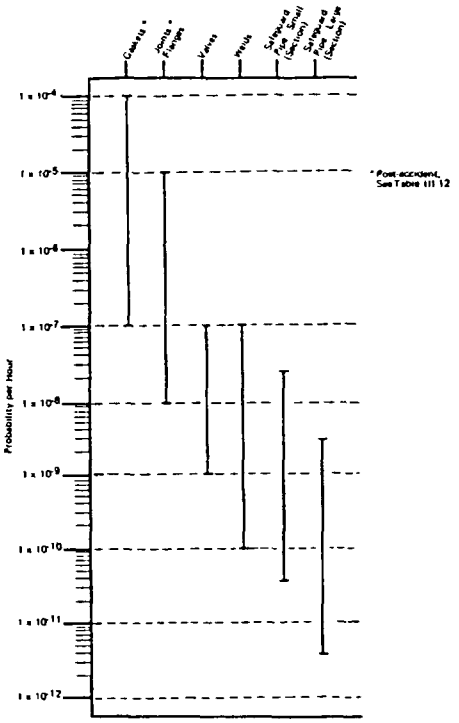


FIGURE III 4-5 Leak and Rupture Assessments for Passive Hardware

Fig. III 4-1 — Fig. III 4-5

Section 5
Test and Maintenance Data and Applications

5.1 INTRODUCTION

Certain test and maintenance acts cause effective removal of a component from the system, rendering it unavailable for some period of time. This unavailability due to test or maintenance is a function of the test or maintenance act duration time and the frequency of the acts. The contribution to the unavailability can be written as:

$$Q = \frac{f(\text{avg acts/month}) \times t_D \text{ (avg hrs/act)}}{720 \text{ (hrs/month)}}$$

where f is the frequency and t_D is the duration time (downtime).

The duration time t_D depends on several factors including the component involved, the complexity of the test or maintenance, the magnitude of repair, contingencies which arise, etc. When maintenance is performed non periodically, f is likewise dependent on similar factors. The log-normal distribution was used to describe the variable nature of these parameters, for the following reasons (in addition to the general considerations discussed in Appendix II):

a. The general agreement found between the log-normal model, and the available test and maintenance data. See Figs. III 5-1 thru III 5-4.

b. The positive skewed nature of the log-normal distribution, which is in accord with the experience that the majority of acts are completed in relatively short times, but that occasionally circumstances require significantly longer times.

c. The capability of defining the distribution and its various parameters from a knowledge of only the assessed ranges. The mean value is pertinent for quantification of the unavailability, and can be obtained from whatever range is assessed, by identifying the limit values with the 5% (X_{min}) and 95% (X_{max}) percentile values and using the relationships given in Appendix II.

Estimates of the maximum and minimum values for the test act and maintenance act durations and frequencies were derived from: 1) discussions with plant test and maintenance teams; 2) analysis of technical specifications (which dictate the maximum allowable outages during powered operation) and; 3) review of maintenance summary reports for four operating plants.

The contributions to unavailability were separated into test contributions and maintenance contributions for four major classes of components: pumps, valves, diesels, and instrumentation.

The bounds which were used to derive mean test durations for the quantification formulas are given in Table III 5-1. The test act includes the minor repair, calibration and reconfiguration time that normally occurs as part of the periodic testing during normal plant powered operation. Those tests that occur during refueling (and other plant outages) do not affect system availability. In general, testing of most safety hardware occurs at monthly intervals; i.e., f (the test frequency) = 1 and the average unavailability due to testing is:

$$Q = \frac{t_D}{720},$$

where

t_D = average (mean) duration time

Maintenance summary reports from Millstone 1 and Dresden 1, 2, and 3 for 1972 provided the data listed on Table III 5-2 for act duration ranges and mean values observed for major corrective and preventative maintenance programs.

The data from which these values were derived are shown plotted in Figs. III 5-1 to III 5-4, along with the theoretical cumulative log-normal distribution derived from the sample mean and variance. The agreement between the model and the data supports use of this distribution as an adequate approximation. (Log-normal probability plots showed similar adequacy in the log-normal fit).

From discussions with plant personnel, it was learned that minor maintenance and repair can occur quite frequently,

and involves short periods of time compared to the more major acts. Furthermore, the plant Technical Specifications restrict in many cases, the duration time that a component within the safeguard system can be "out" for maintenance while the plant is in operation. Certain pumps are limited to 24 hour outages, while others are limited to 72 hours. If the repairs cannot be completed within the allowed interval the plant is placed in a "shutdown" configuration until they are completed. The maximum unavailability of certain components in the event of an accident is thus limited by these restrictions. The maintenance act duration data for most restricted components were therefore derived using 30 minutes and 24 or 72 hour limits. For diesels, because of generally longer maintenance and looser restrictions, bounds of 2 hours and 72 hours were used. These limits and their calculated log-normal means are shown on Table III 5-3.[1]

Finally, frequency of the maintenance act varies from monthly to yearly as indicated by the summary reports; therefore, bounds of 1 month and 12 months were used as the 5 and 95 percentile points on a log-normal distribution to derive the maintenance act frequency values. The mean interval is 4.6 months per act with a range of 1 to 12 months per act. The mean frequency is 0.22 acts per month with a range of 1.0 to 0.083 acts per month.

5.2 CORROBORATION OF THE MODEL RESULTS

To determine the capability of the models to predict unavailability values, the model results were corroborated with the data. The average unavailability from maintenance data was calculated from the individual act duration times listed in the maintenance summary, which were summed over all the components of that class for the year. This value was divided by the number of components of that class in the summary plants to determine an average maintenance act duration per year, and then this value was normalized by the number of hours per year to determine average unavailability, i.e.,

$$Q_{avg} = \frac{\text{Duration of observed acts (hrs/yr)}}{\left(\begin{matrix}\text{Number of}\\ \text{components}\\ \text{per plant}\end{matrix}\right) \cdot \left(\begin{matrix}\text{Number}\\ \text{plants in}\\ \text{summary}\end{matrix}\right) \cdot \left(\text{hrs/yr}\right)}$$

The model results were determined using the equation discussed earlier, i.e.,

$$Q = \frac{f \cdot t_D}{720} ,$$

where t_D and f are the log-normal modeled values previously given.

UNAVAILABILITY

Component	Model Results	Data Results
Pumps	2×10^{-3}	2.5×10^{-3}
Valves	2×10^{-3}	3×10^{-3}
Diesels	6×10^{-3}	1×10^{-2}
Instrumentation	2×10^{-3}	8×10^{-4}

As observed, there is adequate agreement between the theoretical and raw data results.

---

[1] Because of the specifications, the distributions are actually truncated and maintenance times greater than the limit should be set equal to the limit. The log-normal averages account for these truncations.

TABLE III 5-1 SUMMARY OF TEST ACT DURATION

Component	Range on Test Act Duration Time, Hr	Calculated Mean Test Act Duration Time, t_D, Hr
Pumps	0.25 - 4	1.4
Valves	0.25 - 2	0.86
Diesels	0.25 - 4	1.4
Instrumentation	0.25 - 4	1.4

TABLE III 5-2 SUMMARY OF MAJOR MAINTENANCE ACT DURATION (RAW DATA)

Component	Range on Maintenance Act Duration Time, Hr	Mean Maintenance Act Duration Time, t_D, Hr
Pumps	2 - 400	37
Valves	1 - 350	24
Diesels	2 - 300	21
Instrumentation	1/4 - 72	7

TABLE III 5-3 LOG-NORMAL MODELED MAINTENANCE ACT DURATION

Component	Range On Duration Time, Hr	Mean Act Duration Time, Hr
Pumps	1/2 - 24	7
	1/2 - 72	19
Valves	1/2 - 24	7
Diesels	2 - 72	21
Instrumentation	1/4 - 24	6

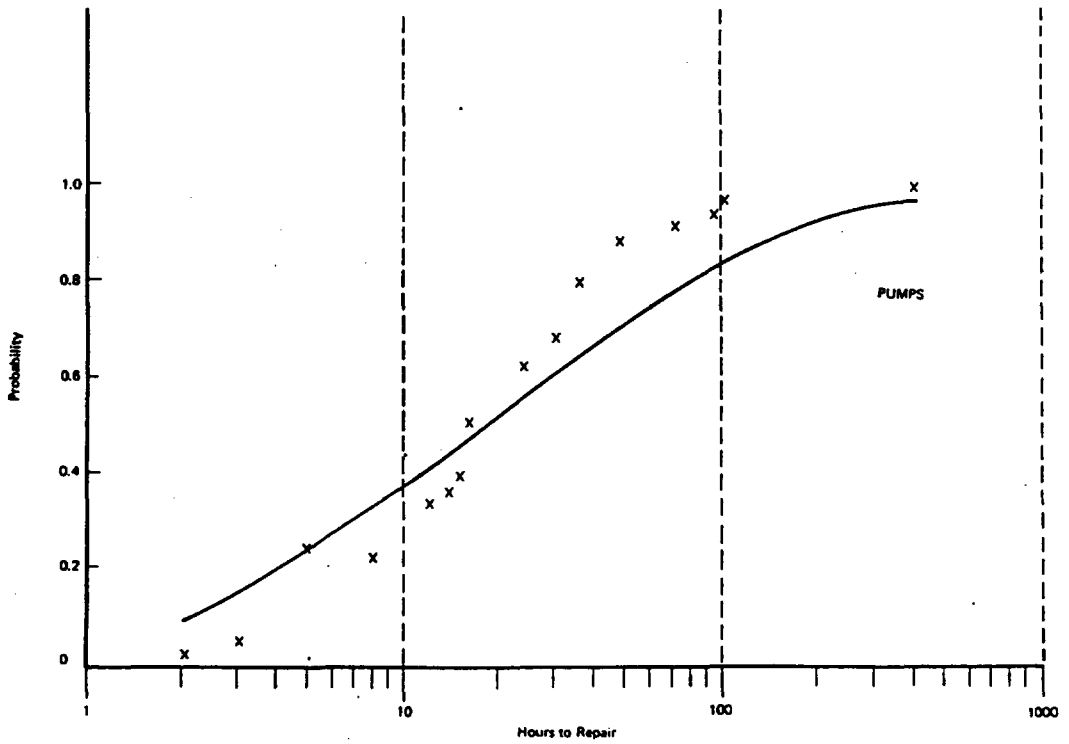


FIGURE III 5-1 Observed Repair Times and Theoretical Distribution - Pumps

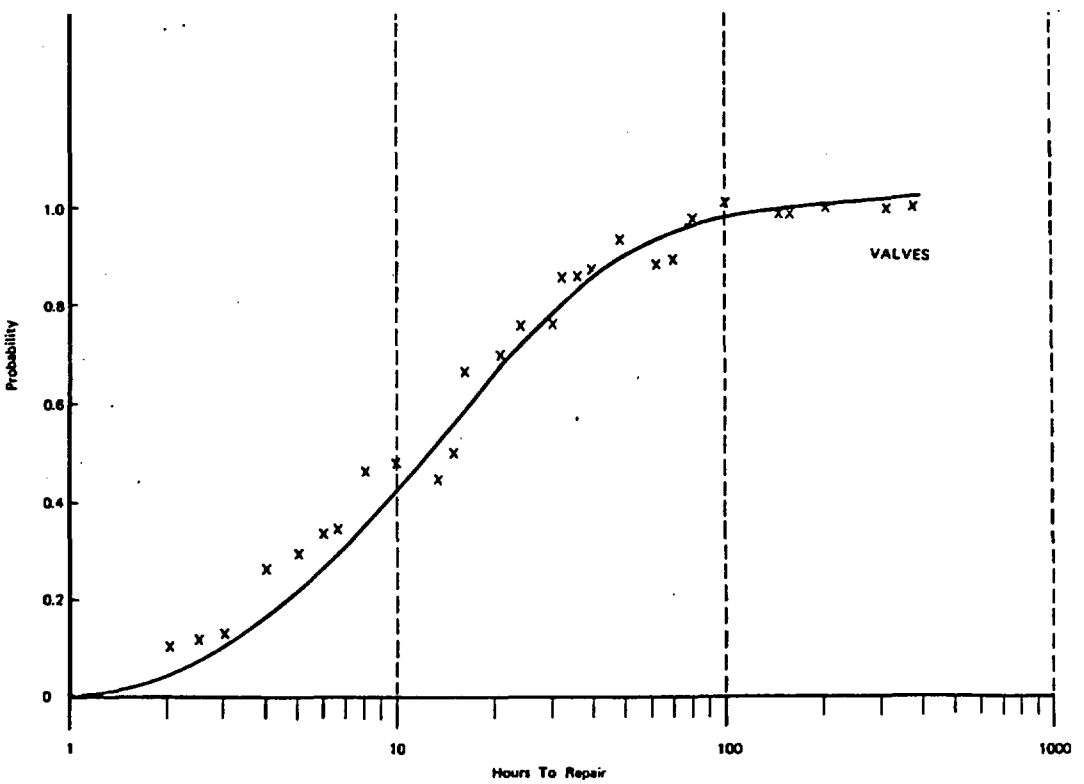


FIGURE III 5-2 Observed Repair Times and Theoretical Distribution - Valves

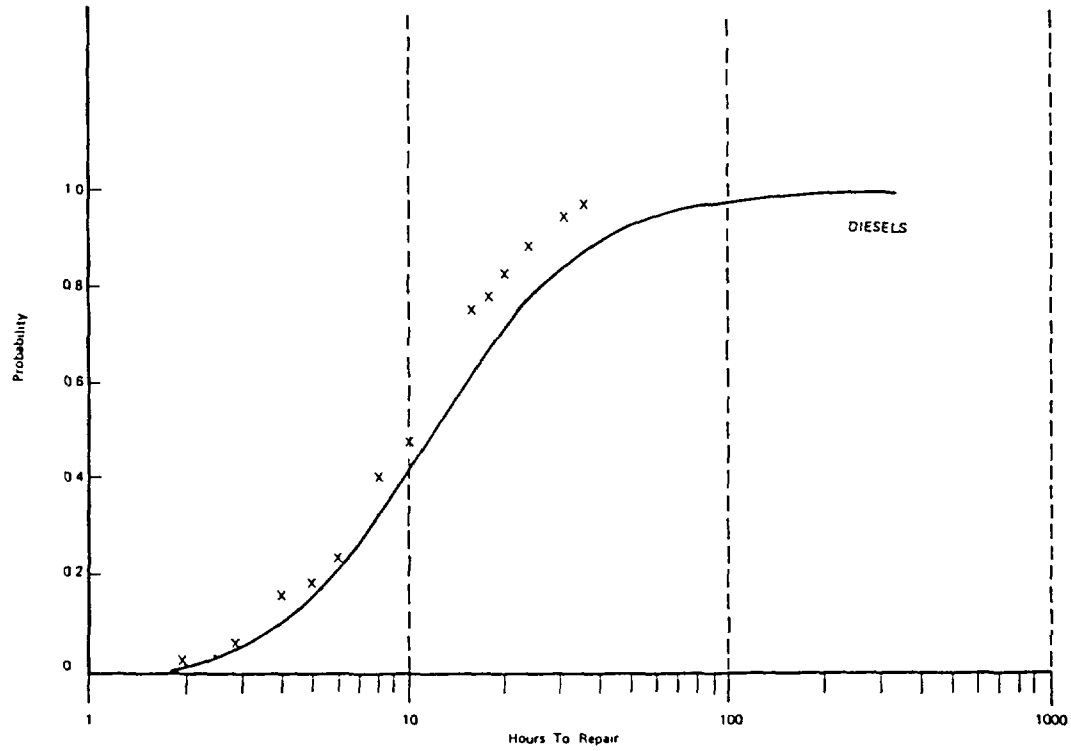


FIGURE III 5-3 Observed Repair Times and Theoretical Distribution - Diesels

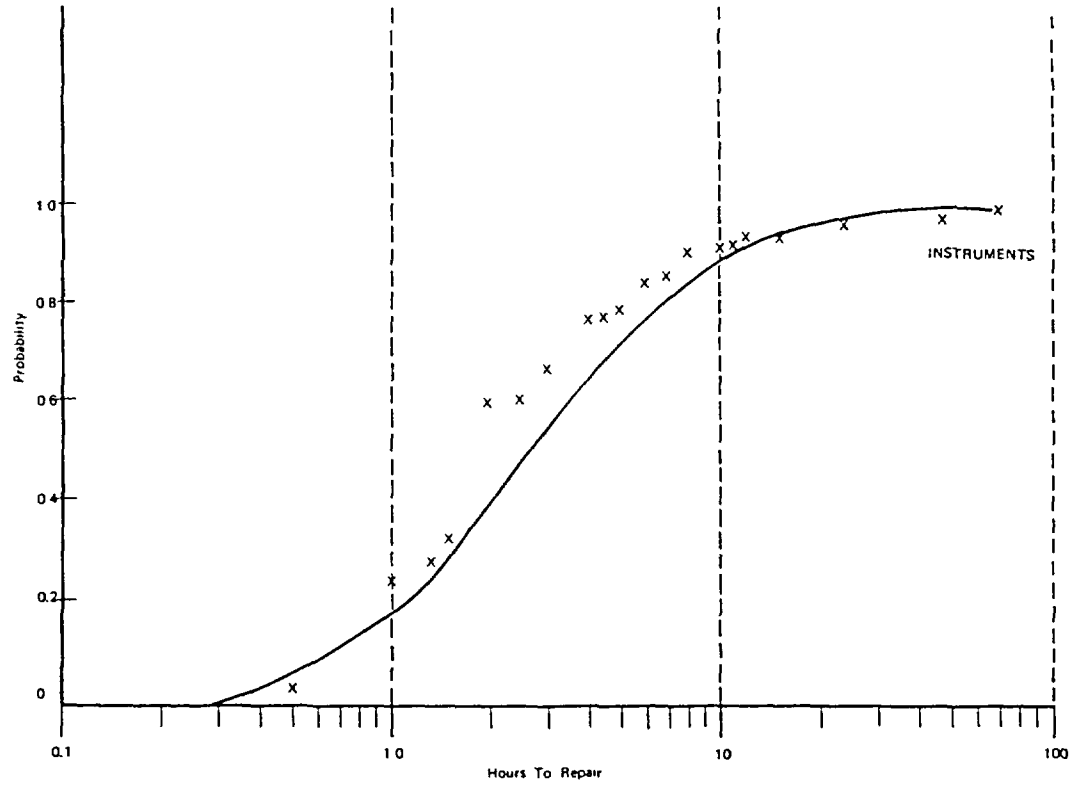


FIGURE III 5-4 Observed Repair Times and Theoretical Distribution - Instrumentation

Fig. III 5-1 — Fig. III 5-4

Section 6
Special Topics

6.1 HUMAN RELIABILITY ANALYSIS

6.1.1 INTRODUCTION

The Safety Systems provided in nuclear power plants to prevent and mitigate accidents are generally designed to operate automatically during the initial states of accident sequences. Information on the conditions in the reactor and on the operation of the Safety Systems during an accident would be displayed at the control room and the operator would be able to follow the sequence of events but no direct human action would be required until the accident is brought automatically under control. There is, however, human interaction with the system in routine plant operation, testing and maintenance. Furthermore human intervention would be required in case of malfunction of automatic systems. Hence, human reliability needs to be considered in safety system analysis.

As an extensive actuarial-type data base does not exist for human reliability, the analysis involves a significant effort in estimation of the reliability of human responses under emergency and normal conditions, and the influence of stress, routine and other factors on error rates for various tasks.

Whenever possible, data were obtained for human reliability in industries involving tasks comparable to those found in nuclear power plants. For some cases data were obtained from military experience, with less similarity to nuclear plant tasks. Because the total available data on the whole are somewhat meager, human reliability analysis as applied to nuclear power plants is still somewhat subjective. Nonetheless, the derived numbers are considered to be sufficiently accurate for risk analysis purposes, with the error bands tending to cover the associated uncertainties.

The human reliability analysis was performed to estimate the influence of human errors on the unavailability of various safety systems and components. Several equally valid approaches can be used to quantify human reliability, and the approach in the study utilized the general features of the THERP Technique for Human Error Rate Prediction, a model developed at Sandia Laboratories (Refs. 1, 2). The model uses conventional reliability technology, describing events in terms of what it calls probability tree diagraming. Probability tree diagraming is simply a form of decision tree or event tree where each step or branch indicates different human actions possible, different environments possible, etc.

In the present study, the system fault trees in Appendix II were analyzed as to the human errors which were combined in the trees. In a number of cases, the human errors were relatively straightforward, and values were directly assigned from basic data considerations.

In other cases, when the human errors were more involved, probability tree diagraming was used to decompose the human error into constituent acts for which basic data existed or for which values could be assigned from extrapolations of basic data. Details of the probability tree diagraming are not given for all the cases analyzed; instead, sufficient information and examples will be given to describe the general technique with data values used and results obtained.

6.1.2 HUMAN PERFORMANCE DATA

An actuarial data base for human error rates in nuclear power plants does not exist. Although the AEC does collect information on human errors associated with abnormal power plant incidents, the data are not generally in a form usable for human reliability analysis. Therefore, in this study, substitutes had to be found for actuarial data. A first data source consisted of human performance data on tasks with similarity to nuclear plant operation, test, maintenance, and calibration tasks. Such data have been compiled for European nuclear reactor operator tasks and also for the process tasks found in petrochemical operations. The sources were the United Kingdom Atomic Energy Authority (UKAEA), the Danish AEC, and the Imperial Chemical Industries, Ltd. (ICI) of Great Britain.

The above sources, though relevant, suffer from lack of actual recorded data. Most of the numbers represent estimates of human error rates based on the judgment of technical personnel in the organizations mentioned. Some data from controlled studies have also been obtained from the UKAEA (Refs. 3, 4) and the ICI (Ref. 5).

A second data source consists of human error rate data from weapons production, maintenance, and testing tasks with less similarity to nuclear plant tasks than the above. These data have been collected by human reliability analysts at Sandia Laboratories. In using these data, the analysts had to judge their applicability to nuclear plant tasks. This judgment accounted for similarity in perceptual, cognitive, and motor aspects of the tasks. It is possible for the equipment involved in the performance of two different tasks to be physically different, and yet for the psychological (behavioral) aspects of the tasks to be similar.

A particular lack of data for the present study concerns the reliability of nuclear power plant personnel after a large loss of coolant accident (LOCA) has occurred. Since there is no historical precedent for this event, there has been no opportunity to see how these personnel would react in the presumedly highly stressful situation created by such an occurrence. In the absence of such experience, the best data available come from studies of man's behavior in other emergency conditions.

Two studies that merit mention here are both considered classics in the area of human factors. In one study by the American Institutes for Research (Ref. 6) critical incidents were collected from Strategic Air Command aircrews after they survived in-flight emergencies (such as loss of engine on takeoff, cabin fire, tire blowout on landing, etc.). The critical incident average error rate was 0.16; that is, 16% of the time the critical actions of the aircrews in such stress situations either made the situation worse or did not provide relief.

In the second study, conducted by the Human Resources Research Organization (Ref. 7) Army recruits were subjected to simulated emergencies such as the increasing proximity of falling mortar shells to their command posts. The recruits were exposed to these simulated emergencies in such a way that they believed the situations to be real. As many as one third of new recruits fled in panic, rather than perform the assigned task that would have resulted in a cessation of the mortar attack. These studies have yielded indications of the devastating effects that very high stress levels can have on the performance of even thoroughly trained, reliable personnel.

In this study, based on the most relevant available data an estimate of 0.2 to 0.3 is assumed as the average error rate for nuclear power plant personnel in a high-stress situation such as a LOCA. This estimate is based on the assumption that the perceived stress in a LOCA situation is comparable to the perceived stress in the two cases studied, whereas it might, in fact, be lower. The human-reliability analysts making this study have judged that the perceived stress would not be higher, so the range of 0.2-0.3 is to be considered conservative.

The average failure rate of 0.2 to 0.3 can thus be used as a rough gauge for average performance of nuclear plant personnel under extreme accident conditions. The value, of course, is simply a rough average value, and, to obtain more accurate evaluations, each particular situation must be individually analyzed to assess the specific human failure rate which is applicable.

Other reported data on stress and human behavior (Ref. 8) indicate that the error rate for a task bears a curvilinear relationship to perceived stress level (see Fig. III 6-1). That is, with very low stress levels, a task is so dull and unchallenging that most operators would not perform at their optimal level. Passive-type inspection tasks are often of this type and can be associated with error rates of 0.5 or higher (Ref. 9). The average error rate of 10^{-1} assigned for less passive monitoring tasks is based on data from the above reference and from reference 10.

When the stress level of a job is somewhat higher (high enough to keep the operator alert) optimum performance levels are reached. But when stress levels are still higher, performance begins to decline again, this time due to the deleterious effects of worry, fear or psychological responses to stress. At the highest level of stress, human reliablity would be at its lowest level, as shown in Fig. III 6-1.

The curve form[1] shown in Fig. III 6-1 has been applied to various tasks in nuclear power plants in determining some of the values in the human error rate data base presented later in this report. For example, the error rate in a typical walk-around inspection of a facility after maintenance is presumed to correspond to an inspector error rate

[1]All figures appear at the end of text.

of 0.5 for a passive inspection task represented on the curve as performance under a "very low" stress level. On the other hand, it is judged that the normal control room situation is sufficiently demanding that performance should be optimal, considering only the effects of stress. Performance after a large LOCA is presumed to correspond to the high error rate (low performance) end of the curve, due to the effects of high stress levels.

Following a LOCA, human reliability would be low, not only because of the stress involved, but also because of a probable incredulity response. Among the operating personnel the probability of occurrence of a large LOCA is believed to be low so that, for some moments, a potential response would likely be to disbelieve panel indications. Under such conditions it is estimated that no action at all might be taken for at least one minute and that if any action is taken it would likely be inappropriate.

With regard to the performance curve, in the study the general error rate was assessed to be 0.9 (9×10^{-1}) 5 minutes after a large LOCA, to 0.1 (10^{-1}) after 30 minutes, and to 0.01 (10^{-2}) after several hours. It is estimated that by 7 days after a large LOCA there would be a complete recovery to a normal, steady-state condition and that normal error rates for individual behavior would apply.

There is an important exception to the shape of the performance curve described. This exception would occur if the operators are called on to take some corrective action after a LOCA and the time available to take this corrective action is severely restricted. One theory of human behavior under time-stress (Refs. 2, 11) holds that the normal error rate for each succeeding corrective action doubles when an error has been made in the preceding corrective attempt or when the preceding action did not have its intended corrective effect. Thus, if one starts out with an error rate of 0.2, theoretically it takes only three more attempts at corrective action to reach a limiting case of an error rate of 1.0. This limiting condition corresponds to an individual's becoming completely disorganized. Extensive clinical experience exists in the literature on human performance to support the theory that large numbers of individuals will fail to perform assigned tasks under severe stress and may become completely disorganized (Refs. 8, 12).

Sufficient data do not exist to determine empirically the exact shape and spread of the distributions of human errors which are directly applicable for nuclear power plant tasks. Therefore, estimates of the human error distribution have been formed with the use of data from other sources.

For the particular shape, a log-normal curve was used in the study, based in part on a Monte Carlo analysis of human performance data (analysis by L. W. Rook, in Ref. 13) and on the time taken to respond to a simulated alarm signal superimposed on normal tasks in a nuclear power plant (Ref. 4). In these studies the human performance curve was found to be skewed, with more performance scores tending towards the low error rates and low response times.

Other studies have yielded curves with shapes that differ in details, but in general the performance curve is skewed toward the higher error rates or response times. In view of the accuracies required for the purposes of the study and the general insensitivity of the overall results to the particular shape used, it is reasonable to assume the log-normal distribution. Therefore, the log-normal distribution which was employed in other areas of study was used for the human error distributions, i.e., the distribution associated with the error ranges and spreads.

Table III 6-1 presents general human error rate estimates derived from existing data (as described above), as modified by the independent judgments of two human-reliability analysts. These judgments were made after reviewing information on nuclear power plant personnel skill levels, previous jobs held by these personnel, operating procedures, and the design of the controls, displays, and other equipment read or manipulated by the operating personnel. The information was obtained in interviews with operating personnel, supervisor, and engineering personnel at nuclear power plants, by observation of control room, test, maintenance, and calibration tasks at several plants, and by a study of written materials and photographs.

As noted in the table, modification of these underlying (basic) probabilities was made as necessary when incorporated into the fault trees. The modifications considered the exact nature of the human engineering, e.g., the close similarity of labeling of different switches, with the attendant higher probability of grasping and manipulating the wrong

switch. A later section describes the application and modification of the basic error rate estimates to a sample human-reliability analysis problem.

In general, human error rates for tasks have been estimated to the nearest order of magnitude, with two analysts making independent estimates based on a detailed description of the task requirements (including written instructions and photographs of controls, displays, valves and other items to be read or manipulated by operating personnel). In all cases, the independent estimates agreed to the nearest order of magnitude. The associated assessed error factors (probability ranges) covered the possible variations and uncertainties associated with the final estimates.

The two specialists attempted to avoid overestimating human reliability, that is, underestimating error rates. Concurrently, they tried to avoid deliberately overestimating error rates to provide only conservative estimates. However, in post-accident situations, e.g., after a LOCA, it was deemed proper to avoid overly optimistic assessments of human reliability.

Some of the estimates were based directly on data collected on tasks identical or highly similar to nuclear reactor tasks. For example, UKAEA experience is that large manual valves that have no readout of their position except the valve itself are left in the incorrect position after non-routine operations approximately once in 100 times (10^{-2} occurrence). Such information was applied in the present study without modification. (This is the case when no special precautions are taken, such as use of padlocks with administratively controlled keys.)

In other cases an analytical approach was necessary to apply existing data on human error rates. In these cases, a nuclear power plant task was broken down into individual steps involving perceptual, conceptual/emotional, and motor aspects of behavior. In more common terms, this means taking a particular step in a task and considering the following three aspects:

1. The inputs to the operator, as provided by such things as displays on control panels, labels, configuration of manual valves (including presence or absence of padlocks), written instructions, and other signals.

2. The thinking and decision making done by the operator is influenced by the interaction of his emotional state (e.g., fear and worry immediately after a large LOCA).

3. The responses the operator makes by means of switches, large valves, oral orders, writing down information etc.

The above analytical approach was used to break down the tasks into smaller bits of behavior that could more readily be combined with existing data or with the experience of the analysts.

Finally, the estimates of error rates for the individual behavioral units were combined into estimates of error rates for larger units of behavior, corresponding to nuclear power plant tasks or groups of tasks. In this recombination operation, the estimated error rates for smaller behavioral units were at times modified in consideration of their interdependencies to avoid the derivation of unrealistically low estimates of task error rates. In the present study, the task error rate estimates so derived were combined with consensus-estimated error rates to enhance the stability of the estimates.

The estimated task error rates were modified, where appropriate, by the effects of available personnel redundancy, that is, the checking of a man's performance by another man. In some cases, the total estimated failure rate of a task, including recovery from an original error made possible by using personnel redundancy, was equal to or less than 10^{-6}. However, experience with human reliability analysis and the observation of "the impossible" have led most specialists in this field to view with skepticism any task error rate less than 10^{-5} for any but the very simplest human acts. Consequently, in the present analysis, estimates of human error rates smaller than 10^{-5} were not used.

The estimates of task error rates were incorporated in fault trees by the fault tree analysts, and human failure events were treated in the same manner as other failure events:

6.1.3 PERFORMANCE-SHAPING FACTORS

Several factors had to be considered in deriving estimated error rates for nuclear power plants. Following are the more important of these factors, each of which is discussed under the topic headings which follow.

- Level of presumed psychological stress

- Quality of human engineering of controls and displays
- Quality of training and practice
- Presence and quality of written instructions and method of use
- Coupling of human actions
- Type of display feedback
- Personnel redundancy

6.1.3.1 Level of Presumed Psychological Stress.

As discussed earlier, the highest error rates were assigned to the time period immediately after a large LOCA, with recovery to normal levels of human reliability occurring as a function of time. Implicit with this assumption that error rates decrease with time is the underlying assumption that things do get better. That is, the nuclear power plant is brought under control with appropriate automatic and manual responses to the emergency.

Normal error rate values have been assigned to routine control room operations and to maintenance and calibration tasks, as it is assumed that the normal stress level has a facilitative effect. In the interviewing and observation of control room operators, maintenance personnel, and calibration technicians, it appeared that the jobs were sufficiently challenging to maintain facilitative levels of motivation. No one seemed bored or "just putting in time". (This is a clinical judgment based on the independent observations of two psychologists trained in clinical evaluations.)

6.1.3.2 Quality of Human Engineering of Controls and Displays.

The basic error rates in Table III 6-1 were modified by assigned higher rates to situations where the arrangement and labeling of controls to be manipulated were potentially confusing. For example, motor operated valves MOV-1860A and MOV-1860B are to be opened at the RWST low level set point (14.5% full). Immediately adjacent to these switches are MOV-1863A and MOV-1863B. The two sets of switch numbers are similar, and they have similar functional labels:

LO HEAD S.I. PP A SUMP SUCT VV

and

LO HEAD S.I. PP A DISC ISO VV

Furthermore, at the low level set point, both sets of valves would normally be closed and the green indicator lamps above them would be illuminated. A sample human reliability analysis using these switches is described in a later section to illustrate how the potential confusion in using these switches can result in human errors.

Fairly high rates were assigned to the probability of manipulating the wrong switch in cases where similar appearing controls and displays were close together without separation by functional flow lines on the panels or some other means to show normal process flow, a design characteristic of operating panels on some research reactors (Ref. 14). In general, the design of controls and displays and their arrangements on operator panels in the nuclear plants studied in this analysis deviate from human engineering standards specified for the design of man-machine systems and accepted as standard practice for military systems (See Refs. 15 through 19). Whether such standards are necessary and would result in a net benefit is outside the goal of this analysis.

It was appropriate to assign fairly low error rates to tasks where the quality of human engineering is such that the cues given for task initiation and correct task completion are difficult to ignore. For example, lower error rates have been assigned to cases where the task initiation cue is an annunciator alarm than where the cue is merely the deviation of a meter on a panel in the control room. Also, for some large manual valves, the use of a special padlock and chain with administratively controlled keys and associated paper work reduces the probability of forgetting to return the valve to the normal condition after maintenance. In the latter case the primary cause of leaving such a valve in the wrong condition after maintenance would be failure to use the required procedures. An estimated 10^{-4} error rate per opportunity was assigned to such failure.

In certain cases, a high recovery factor was assigned to the error of manipulating an incorrect MOV or pair of MOV's. An example of a recovery factor is as follows. Assume an operator is supposed to open a pair of MOV's to increase the flow rate as displayed on a meter. The normal procedure would be for the operator to make the switch manipulation and then observe the flow meter for the proper rate of flow. If the proper rate

of flow fails to materialize, the operator would have a high probability of realizing something was wrong and would likely take corrective action. The example in a later section illustrates some recovery factors.

In general, it was found that most errors in maintenance and calibration tasks either had immediate and compelling feedback of their correctness or incorrectness or that subsequent recovery factors made it highly improbable that errors would remain undetected for long.

6.1.3.3 Quality of Training and Practice.

On the basis of interview, observation, a visit to a training center, and review of training materials, the level of training of nuclear power plant personnel was judged to be outstanding. For example, interviews with control room operators revealed a clear understanding of normal reactor operation. They can readily describe the events occurring in normal on-line operation and have a clear conceptual picture of the processes involved. (In one interview an operator who was considered by his supervisor to be "below average" for operators at the site demonstrated the above thorough understanding.) Therefore, for routine maintenance, calibration, and control room operations, a high degree of trained-in excellence has been assumed with associated high estimates of human reliability.

Although original training includes responses to emergencies, there is no provision for frequent on-site practice in responding to simulated emergencies (such as a large LOCA) at the sites visited. In the absence of appropriate simulation equipment, such on-site practice could be simulated by frequent "talk-through" of responses to emergencies. This type of informal test was made in the course of the present study. It was found that the operators interviewed could explain in general terms what they should do in postulated emergency situations, but they did not always appear to be sure of the locations of switches and readings on displays relevant to manual backup actions required in the event of failure of automatic safeguards systems. This does not imply that, based on such a limited "test" of operator ability in emergencies (i.e., a discussion of a hypothetical situation), operators would not be able to carry out emergency tasks. Nevertheless, the lack of ability to "talk through" appropriate procedures without hesitation or indecision potentially indicates lack of a clear plan of action should such emergency situations occur. Based on the above findings, relatively high error rates were consequently assigned to operator actions required soon after the onset of a major emergency such as a large LOCA.

6.1.3.4 Presence and Quality of Written Instructions and Method of Use.

Generally, a lower error rate was assigned to procedures for which written instructions are available. It was necessary to make an estimate of the likelihood that written instructions would be used by the operator, maintenance technician, or calibration technician, rather than trusting his memory of the procedures. For example, in one of the cases analyzed, even with appropriate use of calibration procedures, it was observed that a technician anticipated what approximate instrument reading should appear for each step in the procedure. He had performed this lengthy calibration procedure so often that he knew what to expect. This knowledge coupled with a very low frequency of finding an out-of-tolerance indication sets up a very strong expectancy that each reading will be in tolerance. Under these circumstances there is some likelihood (estimated as 10^{-2}) that the technician will "see" an out-of-tolerance indication as being in tolerance. (In this particular instance, however, there were so many recovery factors that even with the assumption of a 10^{-2} error rate, the probability of an uncaught and uncorrected calibration error was negligible.)

In estimating error rates, the quality of the written instructions was evaluated. Of concern were such factors as the ease with which an operator could find a written emergency procedure, the extent to which the format would aid the operator, the likely ease of understanding non-routine instructions, and so on. The style of written instructions contributed materially to the estimated error rates. The written instructions do not conform to established principles of good writing; they are more typical of military maintenance procedures of approximately 20 years ago. Other deficiencies which contributed to relatively high error rate estimates were poor printing quality, no distinctive binder or location for emergency procedures, lack of tabs and inappropriate indexing which made it difficult to find specific procedures, and poor format for each procedure.

The observed method of use also contributed to relatively high estimated error rates. Men were observed performing several tasks and then checking them off on the check list. The correct and more reliable procedure would be to perform a listed task, check it off, and then move on to the next item in the check list. Lower error rates were assigned to cases where information from a meter or a dial had to be recorded on the check list rather than merely checking off that an item had been completed. Such a procedure markedly reduces the probability of forgetting to perform a step in the check list.

6.1.3.5 Coupling of Human Actions.

Another important factor is related to the type of grouping of switches or manual valves plus the effects of written instructions. This factor is the amount of coupling of human actions, that is, the relative lack of independence of such actions. Four levels of coupling were used in the analysis: no coupling (i.e., complete independence), loose coupling, tight coupling, and complete coupling (complete dependence). The degree of coupling is assigned on an individual failure basis but some general guidelines were used as illustrated below.

An example of no coupling between tasks would be where the probability of error in one task is independent of the probability of error in another task. Tasks which are dissimilar or which are greatly separated in space and time tend to be independent. However, such tasks might be affected by the same conditions (e.g., the stress after a large LOCA) and the estimates of their error rates were influenced by this consideration.

Loose coupling can be illustrated by two test valves in the PWR containment spray injection system located in a building next to the RWST. Both these large manually operated valves are chained and padlocked in the normally closed position. Periodically they must be unlocked and opened for test purposes. The procedures call for one valve to be opened and that part of the system tested, and then for the valve to be closed, chained, and padlocked before proceeding to open the other valve to test the other part of the system. It was judged there was a small probability that, for convenience, an operator would regard both valves as a unit and not follow the prescribed procedures. That is, he would open both valves prior to any testing and after all testing reclose both valves. Therefore, the probability of forgetting to reclose one valve would not be independent of the probability of forgetting to reclose the other valve. Since most operators would be likely to follow the prescribed procedure, loose coupling best expressed the relationship errors of forgetting for the two valves.

For the valves in question, the important error was forgetting to reclose both valves. The probability of this error was calculated as follows: Generally, loose coupling was taken to be the log-normal median value between the upper and lower bounds. The upper bound on coupling is defined by the assumption of complete coupling between the two acts (i.e. reclosing of the two valves). The lower bound is obtained from the assumption of complete independence between the two acts. Given an estimate of 10^{-2} for the error of forgetting to reclose a single valve, the upper bound becomes 10^{-2} and the lower bound $10^{-2} \times 10^{-2} = 10^{-4}$. The log normal median is the square root of the product of the lower and upper bounds, or,

$$\sqrt{10^{-2} \times 10^{-4}} = \sqrt{10^{-6}} = 1 \times 10^{-3}$$

Thus, the probability of forgetting to reclose each valve is estimated as 10^{-2} and the probability of forgetting to reclose both valves (the only error of importance in the analysis) is estimated as 1×10^{-3}.

Tight coupling can be illustrated by the requirement to calibrate three bistable amplifiers in the reactor protection system (SCRAM). One calibration technician performed the calibration in the instrument room while communicating with an operator in the control room. A 10^{-2} probability was assessed for the error of the technician's miscalibrating the first bistable amplifier, as by using an incorrect set level. The incorrect set level, for example, could be due to a simple misreading error. Given that the calibration technician has miscalibrated the first amplifier, there is a substantial probability of carrying over the incorrect set level to the second bistable amplifier. It was estimated that the conditional probability of miscalibrating the second amplifier, given miscalibration of the first, would be 10^{-1}, or a joint probability of 10^{-3} of miscalibrating both amplifiers. It was estimated that the conditional probability of miscalibrating the third amplifier, given

miscalibration of the first and second amplifiers, would be 1.0, or a joint probability of 10^{-3} of miscalibrating all three bistable amplifiers. In other words, a tightly coupled sequence of events was assumed. In this particular operation, there were several recovery factors, so that the final estimated influence of human errors on the reactor protection system was smaller than the above 10^{-3} estimate for the basic act.

An example of complete coupling is found when one basic act results in several failures. For example, one step in the written procedure calls for the operator to open two valves. The two valves are regarded as one unit by the operator. In estimating the probability of his omitting to open these valves, the same estimated error rate was given for one or both valves. That is, it was considered that if he would open one valve, he would open the other. Likewise, if he failed to open one valve, he would fail to open the other. This analysis is an approximation, of course. Absolutely complete coupling can be very unlikely--yet, in this particular example, it was assessed that human behavior would exhibit high dependency, and complete coupling was assumed as a reasonable approximation.

As a contrast to the above discussions, the following example shows how an apparent common mode error due to apparent coupling was estimated to have no resulting net effect on safety system availability. At one site two possible common mode errors for comparator calibration in the reactor containment pressure consequence limiting system were:

a. using the wrong decade resistance for all channels, and

b. using the wrong scale on the digital voltmeter for all channels.

Once either error is made, the calibration technician might indeed recalibrate an entire rack. The estimated error rate for either common mode error was 10^{-2}. However, when the technician went to the second rack, he would discover that the comparators in that rack, too, needed a gross recalibration, and he should suspect that something was wrong with the test procedure rather than merely proceed to recalibrate the second rack. The estimated failure rate of the recovery factor for the second rack was 10^{-2}. (This estimate was deliberately made conservative.) Since the technician typically calibrates all four racks in one shift, it can be seen that the overall rate of making one of the above two calibration errors and then failing to catch this error and incorrectly recalibrating all four racks is approximately 10^{-2} (the initial error) x 10^{-2} (second rack) x 10^{-2} (third rack) x 10^{-2} (fourth rack), or much less than 10^{-5}. (Recall that we do not use any estimates smaller than 10^{-5}.)

6.1.3.6 Type of Display Feedback.

One of the most important recovery factors to mitigate the effects of an error is the type of display feedback. If an error resulted in an immediate annunciator warning, a relatively low failure rate was assigned to the recovery factors. The total task failure rate would be the product of the initial error rate and the low failure rate of the recovery factor. But if the feedback consisted of a slow rise in pressure, for example, as displayed on a meter on the vertical wall underneath the annunciator panels, a higher failure rate was assigned, in certain instances 0.5.

6.1.3.7 Personnel Redundancy.

Another important recovery factor is the use of personnel redundancy (or, as it is sometimes called, human redundancy) which refers to the use of a second person to verify that the performance of a first person was correct. Personnel redundancy can vary from complete redundancy (i.e., complete independence of the initial act and the checking act) to very low degrees of redundancy (i.e., high degrees of dependency between the initial act and the checking act). Lower recovery factor failure rates are related to higher degrees of personnel redundancy.

Beneficial use of a high degree of personnel redundancy is illustrated by the calibration of the water level sensors and drywell sensors at one site. A two-man team performs the calibration with one man reading and recording the readings on the check list while the other man does the calibration. After the calibration has been completed the two men reverse roles and perform a functional check. With this extensive use of personnel redundancy, an estimate of 10^{-5} was assigned to the joint probability of a miscalibration being made and the functional check failing to catch the miscalibration.

A low degree of personnel redundancy is illustrated by the use of a single person to perform critical actions, followed by an informal type of checking. For example, in the case of

one critical manual valve located at the RWST, one man is responsible for reopening this valve after maintenance. Should he forget to open the valve, the RWST would not be available in the event of a large LOCA. At certain times a walkaround inspection is performed, but (as already noted) the estimated error rate for this type of passive monitoring task is high (0.5).

It is sometimes thought that requiring a person to sign a statement that he has accomplished a task will ensure that he really performed the task. For tasks that are frequently performed, the signing of one's name tends to become a perfunctory activity with no more meaning than checking off an item on a checklist. In general, very little reliability credit was allowed for the requirement to sign off that a procedure had been completed.

In general, the degree of personnel redundancy was high for calibration operations, lower for certain operator tasks such as manipulating MOV's, and lowest for maintenance tasks. However, in the case of the latter, a highly reliable recovery factor was the testing of maintained system components before the system was put back on line.

6.1.4 A SAMPLE HUMAN RELIABILITY ANALYSIS

To illustrate how a typical human reliability analysis was performed, this section outlines a sample analysis based on paragraphs 4.8 and 4.9 of the procedure entitled "Loss of Reactor Coolant," provided by the utility that runs the subject PWR. The two paragraphs are:

4.8 When the RWST reaches the low level setpoint (14.5%) and CLS [Consequence Limiting System] initiation has been reset (RESET PERMISSIVE $\leq$ 0.5 psig) complete the following actions:

- 4.8.1 Open MOV-860A and B, suction to the low head SI [Safety Injection] pumps from the containment sump.
- 4.8.2 Stop the containment spray pump motors and close spray pump turbine steam supply valves MS-103A, B, C and D
- 4.8.3 Close Spray pump suction and discharge valves MOV-CS-100A, 100B, 101A, B, C and D.

4.9 When the RWST reaches the low-low level setpoint (7%) complete the following actions:

- 4.9.1 Close MOV-862, suction to the low head safety injection pumps from the RWST
- 4.9.2 Open the charging pump suctions from the discharge of the low head pumps by opening MOV-863A and B.

This sample analysis is restricted to steps 4.8.1, 4.9.1 and 4.9.2. The MOV switches inovlved are MOV-1860A and B, MOV-1862, and MOV 1863A and B. [NOTE: the procedures drop the initial digit since it is understood, for example, that MOV-860A could refer to this switch for either the number 1 reactor (i.e., MOV-1860A) or the number 2 reactor (MOV-2860A).] These switches are shown in the bottom row of the sketch in Fig. III 8-2. The two rows of switches shown in the sketch are the bottom two rows of seven rows on the left most panel of four segemnts in a large switch board (one plane). There are other safety panels in other planes.

In the sketch the switches are associated with indicator lamps: G stands for green (closed condition of motor operated valve) and R stands for red (open condition of MOV). The lines radiating from some of the indicator lamps indicate the normal "on" condition of these lamps prior to the low level setpoint.

Not shown in the sketch, but of importance to the analysis, is the third row from the bottom of MOV switches. The row consists of 5 switches identical in shape and size to the bottom row. The 5 switches are physically arranged from left to right and are labeled as follows:

LO HEAD S.I. PP A DISC ISO VV MOV-1864A ISO DISC FROM COLD LEGS
LO HEAD S.I. PP A RECIRC ISO VV MOV-1885A
LO HEAD S.I. PP A&B RECIRC ISO VV MOV-1885C
LO HEAD S.I. PP B RECIRC ISO VV MOV-1885B
LO HEAD S.I. PP B DISC ISO VV MOV-1864B ISO DISC FROM COLD LEGS

(Normally open-red lamp)

The procedures in paragraph 4.8 are to be performed about 20-30 minutes after a LOCA, and the procedures in 4.9 should be performed about 2 minutes after those in 4.8. The 14.5% low level setpoint is indicated by a meter that shows dropping water level in the RWST, and also by an annunciator. The 7% low-low level setpoint is similarly indicated.

Reference to Table III 6-1 indicates that the basic operator error rate at the end of 30 minutes after a LOCA is approximately 10^{-1}. This basic error rate was used for certain of the activities as described below.

The first question to be asked in the analysis was: what is the probability that no action would be taken at the low level setpoint condition? The second question was: what is the probability that some pair of switches, other than MOV-1860A and B would be manipulated?

In answering the first question the basic error rate of 10^{-1} was used. However, it was assumed that by 20-30 minutes after a LOCA at least three people would be present in the control room, and that each of these people would have to fail to notice the need for taking action indicated in step 4.8.1. Furthermore, it was estimated that the presence of the meter indication of falling RWST level should add a probability of 0.9 that someone present would be cued to perform step 4.8.1. (This estimate is based on an assumed probability of 0.5 that an individual will fail to notice a change in a meter indication under the circumstances. For three people the joint probability that the change will be unnoticed is $0.5^3 = .125$, yielding a probability of 0.875 that it will be noticed. For convenience, this was rounded to 0.9.) The probability that step 4.8.1 would not be executed is thus estimated as about 10^{-4} prior to the auditory alarm, which would provide another cue for action. This estimate of 10^{-4} is shown in the first branching of the probability tree diagram shown in Fig. III 6-3.

Once the alarm has sounded, the operators have 2 minutes in which to perform step 4.8.1. It was reasoned that if no action has been planned until the alarm sounds, some degree of disorganization is indicated and the basic error rate of 10^{-1} is applicable for each of the three operators. Thus a probability of 10^{-3} was estimated for the failure to take action by any of the three operators within 2 mintues after the first auditory alarm at the 14.5% low level setpoint. This 10^{-3} estimate is shown in Fig. III 6-3 as the second branch leading to failure event F_1. Thus, the total estimated failure rate F_1 (failing to perform step 4.8.1 in time) is $10^{-4} \times 10^{-3} = 10^{-7}$. Although as stated previously an estimated failure rate of less than 10^{-5} should be viewed with skepticism, it can be concluded that the probability of failure to perform step 4.8.1 is relatively small, and this potential failure was therefore dropped from further consideration.

It was estimated that if step 4.8.1 were performed, the probability of selecting some pair of switches other than MOV-1860A and B would be of the order of 10^{-2}. The reliability of this task is estimated at this value because it was assessed to be highly probable that responsibility for operating the valves would be assigned to one person, that is, no personnel redundancy would be used. This judgment was based on observation of operators at work. Misselection of switches is the type of error that operators tend to disregard as a credible error. Therefore, it was deemed unlikely that anyone would check the operator who actually manipulated the MOV's. The basic error rate of 10^{-1} was assessed to be too large for this type of action, and 10^{-2} was accordingly selected as the nearest order of magnitude estimate.

Reference to Fig. III 6-3 indicates that there are two paths leading to misselection of the pair of switches. The path

$$A\text{-}F_2 \left(10^{-4} \times .999 \times 10^{-2} \cong 10^{-6}\right)$$

has a small probability and hence can be rejected. The only remaining failure path of consequence is thus

$$A\text{-}F_3 \left(.999 \times 10^{-2}\right)$$

which reduces to 10^{-2}.

Given that the operator selects a wrong pair of switches at the low level setpoint there now arise the possible candidates of incorrect pairs he will select. It was assessed that the most probable candidates are MOV-1863A and B since they are on the same row of switches, are adjacent to the desired switches, and have similar MOV numbers and labels. The probability of selecting a pair of switches from the second row from the bottom is lower in value because of the dissimilarity of switch nomenclature and the different appearance of the switches themselves (they

have an AUTO position). The switches in the third row from the bottom have labels similar to the desired switches, but the outboard switches (the most likely candidates for mis-selection) are normally open. Their red-indicator lamps would furnish a cue that they are not the correct switches to be manipulated. In addition, this third row is spatially somewhat remote from the desired switches.

Given the initial error of selecting some pair of switches other than MOV-1860A and B, it is therefore estimated that there is a probability of .75 that the operator would select MOV-1863A and B and a probability of .25 that some other pair of switches would be selected. The error of mis-selection of MOV-1863A and B has a recovery factor which enters at the 7% (low-low) level setpoint. That is, in step 4.9.2 the operator is supposed to close MOV-1863A and B. If the error of mis-selection had already been committed, the operator would find these MOV's already closed. This situation will likely cue him that something is wrong. A 0.9 probability is therefore used for his noting an error, and hence the total estimated failure rate for step 4.8.1, including failure of the recovery factor, is $10^{-2} \times 0.75 \times 10^{-1} = 0.00075$ which is rounded to approximately 10^{-3}.

A similar analysis was performed for steps 4.9.1 and 4.9.2. The detailed analytical approach described above involves a degree of subjectivity. For the study this subjectivity was not particularly crucial because what is important and affects the overall results is the order of magnitude of the human error failure rate and not its exact value. The error bounds attached to the final estimate also gave coverage to uncertainties and errors which might exist. As a tool in itself, the detailed analytical approach is valuable for the following reasons:

a. The exercise of outlining all plausible modes of operator action decreases the probability that some important failure path will be overlooked.

b. Due to the lack of error rate data for nuclear power plant tasks, it is necessary to break down operator actions to a level where existing data can be used.

c. The detailed approach makes it easier for analysts making independent estimates to check on the source of any disagreement and to resolve it.

6.2 AIRCRAFT CRASH PROBABILITIES

The AEC Regulatory Staff has compiled data (Refs. 20, 21, 22) on aircraft movements and calculated crash probabilities as a function of distance from an airport and orientation with respect to runway flight paths. The probabilities are computed per square miles per aircraft movement so that the individual plant sites can be evaluated by determining the plant vulnerable area, distance from the airport and the number of aircraft movements involved. Table III 6-2 which was taken from Reference 23 is based on general aviation aircraft movements for the years 1964 through 1968 and includes 3993 fatal crashes as a result of 320,000,000 aircraft movements. Only crashes resulting in a fatality were considered. It is reasonable to assume that accidents severe enough to create significant damage to a nuclear plant would generally involve fatal injuries, however.

Table III 6-3 presents fatal crash histories of air carrier and military aircraft. Crashes within ten miles of an airport runway and within a 60 degree reference flight path symmetric about the extended center line of the runway are considered.

Although the number of aircraft movements per year may increase significantly in the next four decades, the fatal crash probability per aircraft movement per square mile is expected to stay relatively constant and will probably decrease as safety technology develops in future years. The updating of the crash probabilities to account for future growth can then be accomplished by estimating the increase in aircraft movements for the period of concern. A study conducted by Sandia Laboratories indicates that the accident rate per mile for all U.S. air carriers steadily decreased over the period of 1968 through 1971 even though the number of miles flown increased significantly.

It is reasonable to expect this trend to continue so that extrapolation of crash probabilities based solely on the expected increase in aircraft movements will result in conservative answers.

Based on the reference data on the probability of aircraft crashes as a function of number of aircraft movements and

vulnerable area, the analysis of specific plants is dependent on (1) the number and nature of aircraft movements in the vicinity of the plant, (2) the vulnerable area of the plant and (3) the damage potential of aircraft crashes into the vulnerable area.

6.2.1 NUMBER AND NATURE OF AIRCRAFT MOVEMENTS

Aircraft movements considered have generally been limited by size or weight restrictions. The assumption commonly made is that aircraft having a weight of 12,500 lbs. or greater will cause serious damage to a reactor plant. It is assumed that some portion (25% for Surry) of the smaller aircraft is large enough to cause damage. Judgements on size and speed considerations are made for individual airport-plant interactions based on the type of aircraft involved.

6.2.2 DETERMINATION OF PLANT VULNERABLE AREA

The plant vulnerable area is calculated as the "shadow" area in square miles of vulnerable plant structures based on a defined impact angle. The angle is generally assumed to be 20° although it may vary from 10° to 30°. It should be noted that the effective area will vary depending on the direction of approach, terrain features, and type of damage.

6.2.3 DAMAGE POTENTIAL

Two types of damage are generally considered, (1) fire damage either from the aircraft exploding and burning or from sprayed fuel igniting, and (2) structural damage due to impact of the aircraft frame and engines.

Table III 6-4 was taken from Reference 23 and shows the calculated probabilities for three plants. The table has been expanded to include the Surry plant Units 3 and 4. The information for Surry was taken from the Safety Analysis Report and from the AEC Regulatory Staff evaluation.

6.2.4 TYPICAL DAMAGE CALCULATIONS (SURRY 3 and 4)

6.2.4.1 Source.

a. Felker AAF Field

Five miles SE of the site.

Maximum gross weight of aircraft = 47,000 lb.

1972 number of operations = 81,500.

b. Assumed Conditions:

1. Only 1/2 of the 81,500 operations fly over the site. (Since 1/2 are landings and 1/2 are takeoffs, it is likely that only one or the other and not both types of operation would be involved.)
2. Half of the operations are by large aircraft and half by smaller aircraft (less than 12,500 lb.).
3. Of the smaller aircraft, only 1/4 are large enough to cause damage.
4. Vulnerable areas of each unit are less than 0.01 mi^2 and 0.005 mi^2 for large and small aircraft respectively.
5. Probability of fatal crash is less than $0.3 \times 10^{-8}/mi^2$ per operation. (Military aviation has a better safety record than general aviation.) Accordingly, the probability of an aircraft accident resulting in structural damage is:

$$P_{S,A} \leq \frac{<81,500}{2} \times \frac{1}{2} \times 0.01 \times 3 \times 10^{-9} + \frac{81,500}{2} \times \frac{1}{2} \times \frac{1}{4} \times 0.005 \times 3 \times 10^{-9}$$

$$P_{S,A} \leq 7 \times 10^{-7}/\text{year}$$

6.2.4.2 Source.

a. Williamsburg - Jamestown Airport

Five miles N-NW of the site.

Maximum gross weight of aircraft = 12,000 pounds.

1972 number of operations = 45,000.

b. Assumed Conditions:

Using a probability of crash of $1 \times 10^{-8}/mi^2$ and assuming that only 1/4 of aircraft are large enough to cause damage since this is a relatively small airport with predominately light aircraft traffic.

$$P_{S,B} \leq \frac{45,000}{2} \times 0.005 \times 1 \times 10^{-8} \times \frac{1}{4}$$

$$P_{S,B} \leq 3 \times 10^{-7}/\text{year} .$$

To determine the likelihood of an impact of the containment vessel the ratio of the containment vessel area to the overall target area was estimated at 0.5, which results in a probability of 5×10^{-7} for impact on the containment structures.

Further, in Reference 23, it was concluded the likelihood of a penetration (given impact) resulting in damage to a critical element within the containment vessels (such as the reactor, the primary piping, etc.) was reduced at least a factor of 100. Therefore, the estimate of critical damage due to an aircraft accident is conservatively established at:

$$P < 5 \times 10^{-9}/\text{plant year} .$$

6.3 TOTAL LOSS OF ELECTRIC POWER

An event of major concern in the reactor safety study is total loss of electrical power at LOCA or during the course of a LOCA. Accordingly, the statistics and methodology used to quantify the likelihood of such an event are reported herein.

This event requires the failure of two essentially independent systems, the offsite power system and the onsite power system. Further, because the electrical requirements are reduced as time progresses subsequent to a LOCA, the event was evaluated for two discrete time periods: (1) at the instant of a LOCA; (2) at time periods up to nine months after a LOCA, provided that the electrical system operated properly at LOCA.

Because time is not a factor for loss of electric power at LOCA, cyclic or per demand statistics were used to compute the probability of such a loss in lieu of the more standard failure rate data. Conversely, because time is a factor for loss of electric power during the course of a LOCA, applicable failure rates were used to compute the probability of such a loss.

6.3.1 TOTAL LOSS OF ELECTRIC POWER AT LOCA

The sequence that leads to this event is loss of the offsite power sources at LOCA, and the subsequent failure of the diesel generators to start or to pick up load. The Technical Specifications do not permit operation of the reactor without offsite power. Therefore, offsite power is assumed to be available immediately prior to a LOCA. Since the time frame of interest for this event is in the order of one minute, the likelihood of losing offsite power by a failure which is not causally related to the LOCA is negligible. Likewise, because of the short time span, credit cannot be taken for corrective actions during this event.

A LOCA will cause a generator trip, resulting in a sudden loss of generation. If this sudden loss of generation exceeds the transient stability limit of the power system, then offsite power will be lost. The Federal Power Commission has provided transient stability information for power plants east of the Rockies. Based on this information, the probability is assumed to be 10^{-3} that offsite power would be lost as a result of the generator trip that would arise from a LOCA. This is the value used in this study, although for the particular plant considered in this study, this number might be lower (i.e., the transmission system of the plant reviewed has a high transient stability limit due to high installed capacity, the extensive grid interconnections with other large utilities, and the number of 500 and 230 kV transmission lines connecting the plant to the grid). Conversely, this number would be higher for other areas, e.g., Florida, where the transient stability limit is relatively low. The associated error spreads serve to cover such possible deviations.

If offsite power is lost at LOCA, then the subsequent loss of two diesel generators results in total loss of electric power at LOCA. Both diesels could either fail to start, or both generators could trip due to the sudden application of load. Either case, failing to start or tripping, would result in total loss of power. The failure of both diesels to start is considered to be a random event due to two independent failures. Nuclear operating experiences (the data tables) indicate that the failing to start probability is 3×10^{-2} per demand. Since two diesel generators are involved, the probability that both fail to start is 9×10^{-4}, or approximately 10^{-3}. If both diesels start, the subsequent tripping of both generators would result in total loss of power at LOCA. Since both generators must pick up all emergency loads upon loss of offsite power, this is a single event that could trip both units. Based on analyses and sparse engineering data, the probability

of such an event is assessed to be 10^{-2}, compared to 10^{-3} for independent failure calculation (Ref. 24 through 27). The error spreads again serve to cover the associated variabilities of this estimate.

The loss of offsite power at LOCA, (q_{net}), was estimated to be 10^{-3}, and the loss of both diesel generators, (q_{2DG}) was governed by the tripping sequence and estimated to be 10^{-2}. Since offsite power and onsite power must be lost to cause total loss of power at LOCA, the point probability of such an event, (q_{AC}) can be computed as follows:

$$q_{AC} = (q_{net})\ (q_{2DG}) = 10^{-3} \times 10^{-2}$$

$$= 10^{-5}\ .$$

Because the ESF requirements are most stringent immediately after a LOCA (e.g., the core would be uncovered in a matter of minutes without electric power), no credit is taken for remedial actions such as restoration of offsite power or manual start or repair of diesel generators.

6.3.2 TOTAL LOSS OF ELECTRIC POWER DURING A LOCA

A premise for this event is that power was available at LOCA and that the subsequent total loss of power was due to random uncorrelated events. As in the case of total loss of electric power at LOCA, this event requires the loss of offsite and onsite power. In contrast to the case of total loss of electric power at LOCA, this event allows credit to be taken for corrective actions. Credit for corrective action is allowed because the requirements of the ESF systems, primarily the heat removal system, become progressively less stringent as time passes after the LOCA.

The probability of this event therefore involves two aspects: (1) reliability, (2) maintainability. The reliability aspect is the probability that the total electric power system will fail at some time, T, after the LOCA; the maintainability aspect is the probability that power cannot be restored before the maximum allowable outage time (i.e., the time required to uncover the core). Thus, the relevant probability for this event is the joint probability that all power is lost and that it is not restored before the maximum allowable outage time.

Vendor data indicate that the time required to uncover the core upon loss of all electric power, τ_{max}, can be approximated by a linear function whenever the time t after LOCA exceed 144 hours;

$$\tau_{max}\ (t) = 0\ ; \qquad t < 144\ hr$$

$$\tau_{max}\ (t) = 1 + \frac{t}{720}\ ;\ t \geq 144\ hr$$

Thus, all electric power may safely be lost for approximately two hours in the period starting one month after a LOCA occurrence. As a result, the repair models used for restoration of electric power allow a maximum repair time which coincides with the above equations.

The computed maximum allowable outage times were subsequently coupled with applicable repair data, and the probability of not restoring power within the maximum allowed outage time was determined. The cumulative probability of losing all power increases directly with time; however, because the time allowed to repair such outages also increases with time, the cumulative probability of meaningful failures increases less rapidly than would otherwise be the case.

The data on which the probability calculations are based include nuclear operating experience for loss of offsite power and diesel failure and repair, and utility operating experience for restoration of offsite power. Nuclear operating experience for 1972 includes three events where offsite power was lost.

These events occurred in about 150,000 operating hours, giving a point estimate of the failure rate for offsite power, λ(net), of 2×10^{-5} failures per hour. This data was not inconsistent with the other experiences.

The repair model for restoration of offsite power was based on outage data of the Bonneville Power Administration for the years 1970, 1971 and 1972. The statistics represent the operating experience of more than 11,000 miles of transmission lines rated at 500, 345, 287, 230, 138 and 115 kV, and include more than 1500 outages. These statistics are summarized in Tables III 6-5, 6-6, 6-7. These data represent single failures, and not necessarily the loss of offsite power; however, the repair data are applicable because the repair of a single line would constitute restoration of offsite power. For the outages reported, the restoration time

ranged from more than 150 hours to essentially zero time. A cumulative distribution curve of these outages was plotted (Fig. III 6-4), and the mean repair time was found to be less than 0.25 hour. For the post-accident environment, a conservative, constant mean repair time (τ_{net}) of 1 hour was used. Thus, the probability that offsite power is not returned to service by time t after failure is approximated by exp ($-t/\tau_{net}$). As shown in the tables, the outages are caused by such factors as trees in line, lightning, storm, fire, malicious damage, accidental damage and fire. The major contributor to the total number of outages is lightning, and the outages which require the longest time to repair are generally those associated with fire, ice or line material failures. To better depict the distribution of these outages, a histogram was plotted on semi-log paper, Fig. III 6-5.

The data were in the form of numbers of incidents and total outage times within each cause category. Although this pre-averaging may distort details of the distribution (i.e., all incidents of a given type are assigned the same average outage time) the conclusions are not sensitive to it. The distribution in Fig. III 6-4 bears a reasonable resemblance to a log-normal curve, and the mean repair time used in further calculations was assessed to be adequate for the purposes of the study.

As previously stated, the probability that both diesels fail to start independently is approximately 10^{-3}. However, if the diesels are required to pick up a significant load immediately after start, as is the case, the probability that both generators will trip out, q(2DG), is 10^{-2}. Data for repair of diesel generator sets were not very detailed. For the study's purposes, however, the 1972 nuclear operating experience data were able to be used to estimate the mean repair time, τ_{DG}, of the diesel generators, which was twenty-one hours.

Total loss of electric power during the course of a LOCA involves the loss of offsite power with both diesels failing to pick up load, and neither the offsite power source nor any diesel being repaired before the maximum allowed outage time, τ_{max}, has elapsed. The cumulative probability for this combined event can be given by the following equation:

$$p(t) = \int_o^t \lambda_{(net)} dt' \exp\left(\frac{-\tau_{max}(t')}{\tau_{net}}\right) q(2\ DG) \exp\left(-2\ \frac{\tau_{max}(t')}{\tau_{DG}}\right)$$

$$= \lambda(net)\ q\ (2\ DG)\ t,\ t<t_o$$

$$= \lambda(net)\ q\ (2\ DG) \left\{ t_o + \frac{\tau}{\tau'} \left[\exp\left(-\frac{\tau'\ t_o + 1}{\tau}\right) - \exp\left(-\frac{\tau'\ t + 1}{\tau}\right)\right]\right\}$$

where

$$t_o = 144 \text{ hrs}$$

$$1/\tau = 1/\tau_{net} + 2/\tau_{DG} = 1.095$$

$$\tau_{max}(t) = \tau' t + 1$$

$$\tau' = 1/720$$

$$\lambda(net) = 2.0 \times 10^{-5}$$

$$q\ (2\ DG) = 10^{-2}$$

6.3.3 SUMMARY

The probability of total loss of electric power was computed for two discrete time periods: (1) at LOCA and (2) during the course of a LOCA. The results are tabulated as follows:

a. Total loss of electric power at LOCA, $Q_{med} = 10^{-5}$ per demand. The 90 percent probability bounds (range) on this median estimate are:

$Q_{lower} = 10^{-6}$ per demand;

$Q_{upper} = 10^{-4}$ per demand.

b. The point estimates of total loss of electric power during a LOCA, given

success at LOCA, and the associated 90 percent probability bounds for various times after a LOCA (see Table III 6-8) were computed by using the aforementioned equation and by including the relatively small contributions from other fault tree analyses. (The point estimates were taken as median values with regard to the probability bounds.)

6.4 PIPE FAILURE DATA.

The probabilities of pipe failure as an initiating event for loss of coolant accidents are listed in Table III 6-9.

The pipe rupture assessments noted in Table III 6-9 were obtained from examination of nuclear data sources, industrial data sources, and a number of other data sources. The same type of range approach as used for the component data base was used for the pipe rupture assessments. Each of the various data sources was individually evaluated to obtain pipe rupture assessments. Ranges (i.e., error spreads) were then determined which covered and were not inconsistent with the individual estimates yielded by the various sources.

In general, the pipe data from the various sources were quite rough and gave much freedom of interpretation. To incorporate the resulting uncertainty and possible variations that could exist in the assessments, the ranges (error spreads) were required to be large in size. As with the other data, the associated median values represent the geometric midpoint of the ranges; the associated error factor from median to range endpoint is thus 10. The range, or error spread, and median values are again rounded to the nearest half value on the exponent scale. For error determination, a log normal was assigned to the above ranges and the ranges were interpreted at 90% probability.

Various pipe sizes were included in the evaluations and the rupture data were categorized into different sizes. In general, the basic pipe data, as given in the data sources, could be broken into two general categories, ruptures occurring in pipes less than roughly 4" in diameter and ruptures occurring in pipes having diameters greater than 4". In the summaries of the individual data sources which will be presented, the data are broken into these two categories for analyses where the less than 4" diameter pipes are simply termed "small pipes" and the greater diameter ones, "large pipes".

For the final assessments, the rupture data were extended and interpolated into three categories as shown above. This finer categorization was done principally for modeling considerations and is somewhat subjective, based on judgement and on extrapolation of general trends observed in the basic data. The finer structure is not inconsistent with the basic data and the two group classifications; the highest and lowest bounds (10^{-2} and 10^{-5}) agree with the two groups and the total range which is obtained from the basic data. The large ranges stemming from basic data which are associated with each category tend to cover any categorization errors made and any categorization variation which can occur, with the range sizes causing all the categories to overlap heavily one another.

In addition to the pipe sizes, the rupture size and severity varied over a spectrum, which contributed to the uncertainty. In general, ruptures were categorized as those breaks of major, severance-type size. Minor leaks were not counted in the rupture assessments. When there were questions concerning particular failures, evaluations were performed both including and excluding these failures which served in determining the ranges for the assessments.

The assessments made in the study apply to those types of pipe ruptures which would cause LOCA's. When data sources were in the form of total, per plant probabilities that were applicable to a rupture occurring in systems anywhere in the plant, these total probabilities were normalized by the ratio of LOCA sensitive piping to the total piping in which failures were reported. Average plant characteristics were used to determine the fraction of piping in the data base associated with possible LOCA initiation; the characteristic values used are shown below, followed by the evaluation of the individual data sources. The variation in these characteristic values from plant to plant was judged to be negligible compared to the assessed ranges associated with the basic data variability.

Finally, event trees were constructed to analyze additional, plant-peculiar causes of rupture which were not included in the data histories which were examined. These additional causes were then incorporated along with the data assessment values in the final risk evaluations.

6.4.1 PLANT PARAMETERS

Average characteristics are listed as follows:

a. LOCA Sensitive Piping - 10% of total piping in the reported data base.

b. LOCA Sensitive Small Piping - 4.7% of total piping in the reported data base, 10% of small piping.

c. LOCA Sensitive Large Piping - 5.3% of total piping in the reported data base, 10% of large piping.

From the average plant characteristics, approximate relations are obtainable between total plant failure rates and failure rates for the LOCA sensitive piping. If failures are recorded for the total plant, then:

$$\left(\begin{matrix}\text{Large Pipe LOCA}\\ \text{Rupture Rate}\end{matrix}\right) = \left(\begin{matrix}\text{Rupture Rate for}\\ \text{Total Plant}\end{matrix}\right) \times 0.047$$

$$\left(\begin{matrix}\text{Small Pipe LOCA}\\ \text{Rupture Rate}\end{matrix}\right) = \left(\begin{matrix}\text{Rupture Rate for}\\ \text{Total Plant}\end{matrix}\right) \times 0.053$$

If the failures are broken into those occurring in large piping and in small piping, then the respective rates are multiplied by 0.10 to obtain the LOCA rates:

$$\left(\begin{matrix}\text{Large Pipe LOCA}\\ \text{Rupture Rate}\end{matrix}\right) = \left(\begin{matrix}\text{Rupture Rate for}\\ \text{Large Piping}\end{matrix}\right) \times 0.10$$

$$\left(\begin{matrix}\text{Small Pipe LOCA}\\ \text{Rupture Rate}\end{matrix}\right) = \left(\begin{matrix}\text{Rupture Rate for}\\ \text{Small Piping}\end{matrix}\right) \times 0.10$$

The aforementioned relationships assume a uniform occurrence of failure with regard to pipe location. For order of magnitude calculations the relationship is reasonable if the error spreads are large enough to incorporate any errors made in this extrapolation. For the total plant rate relationships, each factor (i.e., 0.047 and 0.053) is approximately 0.05, which is a factor of two different from the large and small breakdown fractions of 0.10. For order of magnitude calculations, this difference is generally not significant. In the following data source summaries, λ(LPB) will be used to represent the large pipe LOCA rupture rate ($\gtrsim$ 4") and λ(SPB) will be used to represent the small pipe LOCA rupture rate ($\lesssim$ 4").

6.4.2 NUCLEAR AND NUCLEAR-RELATED EXPERIENCE

In approximately 150 reactor years of commercial nuclear power plant experience to date, there have been no catastrophic failures of the primary coolant loop. A crack in the secondary loop was recorded, believed due to a water hammer effect; however, complete severance did not occur. Using 1 failure as an upper bound, therefore,

$$\lambda(\text{LPB}) \leq \frac{1}{150} = 7 \times 10^{-3}/\text{plant year} .$$

Essentially the same result is obtained if zero (0) failures are used and a 95% chi square (or Poisson) confidence bound is taken ($\lambda(\text{LPB})_{95\%} \leq 3/150$). The bound is high, not particularly due to the actual failure rate being high but to lack of sufficient data.

If one interprets the above values as applying to the large piping of the entire plant, then the 7×10^{-3} value can be multiplied by the LOCA sensitivity factor (susceptibility) of 0.10 to obtain another bound for λ(LPB).

$$\lambda(\text{LPB}) \leq 7 \times 10^{-3} \times 0.10$$

$$\leq 7 \times 10^{-4}/\text{plant year} .$$

With regard to small pipe ruptures, the same type values as above are also obtained. Several failures have occurred, none of which were complete ruptures, and there is freedom as to precise applicability and failure counts. Using 1 failure as an order of magnitude type value,

$$\lambda(\text{SPB}) \leq 7 \times 10^{-3}/\text{plant year} .$$

Extrapolation to the small piping of the entire plant as before will yield an additional factor of 10 reduction.

The above values represent gross order of magnitude type bounds, which are dominated by lack of sufficient and precise data. Because of the associated uncertainties, attempts to categorize the history in more detail, by subjective judgement, will yield no further significant information with regard to the overall statistical assessments.

If the experimental reactor experience and military applications experience (naval) are added to the commercial nuclear experience, then additional values can be obtained. There are approximately 40 odd years of experimental reactor experience and on the order of 1200 reactor years of military experience. Including this experience with the approximately 150 years of commercial experience gives on the order of 1400 years of combined nuclear experience.

In the 1400 years of total experience there have been no reported large pipe ruptures occurring in the primary loops. Using 1 failure as an upper bound, which within the accuracies being computed agrees with the 95% zero failure bound, one obtains

$$\lambda(\text{LPB}) \leq \frac{1}{1400} = 7 \times 10^{-4}/\text{plant year} .$$

In the above calculation, a plant year is taken to be synonymous with a reactor year. The 10% LOCA sensitivity factor can be applied to obtain another order of magnitude reduction; however, since the data are not directly correlated with plant characteristics, the 10% factor adds extra uncertainty. Precise small pipe rupture data were not available; however, the same order of magnitude value as above, i.e., 10^{-3}, would be roughly applicable, the value being less conservative with several failures being counted for the bound.

In addition to the bounds obtained from commercial experience and combined nuclear experience, rough bounds can also be obtained from non-rupture failure data on process piping. Rupture probabilities are obtained (extrapolated) from the non-rupture statistics by applying non-rupture to rupture detection (severity) factors. Process piping does not necessarily have the same failure characteristics as the better quality coolant piping, the LOCA related piping, which causes additional possible conservatism and uncertainty to be included. Since the bounds are to be interpreted as rough indicators, the effects will not impact the bound applications.

Using the 1972 nuclear history examined for the general data base, the process piping failures can be grossly categorized as follows:

a. Process Piping Failures (17 plants)

   4 Breaks (severity lying between minor leakage and major rupture)

   4 Minor leaks

b. Other failure related occurrences

   1 Pipe dented - no break

   1 Pipe hanger failure - no resulting damage

The pipe sizes are not separated since the detection, or severity factor, will serve to differentiate large and small rupture probabilities. The above data are taken from the more detailed tabulations given in the general data base discussion.

Rate of breakage in large LOCA-sensitive piping (per plant per year):

$$= \frac{4}{17} \times 0.047 = 1.0 \times 10^{-2}$$

Since the amount of small piping is approximately equal to the amount of large piping, the rate of breakage for small LOCA sensitive piping will also be approximately 1.0×10^{-2}. This breakage rate can then be taken as an upper bound for the small pipe LOCA rupture rate:

$$\lambda(\text{SPB}) \leq 1.0 \times 10^{-2}$$

If a fraction of the breakage rate is taken as advancing to large ruptures, then the upper bound will be reduced by this fraction to obtain the large pipe rupture rate. In terms of experience data, this severity fraction is the ratio of large ruptures occurring to the number of breakages occurring. The severity fraction represents a detection inefficiency and can be taken as incorporating the probability that a rupture will occur without intermediate leakage or breakage.

Using the average empirical value of 0.05 from the G.E. and English data (given in their associated data assessments), which represents a 95% detection efficiency.

$$\lambda(\text{LPB}) \leq 1.0 \times 10^{-2} \times 0.05$$

$$\leq 5 \times 10^{-4}$$

6.4.3 U.S. NON-NUCLEAR UTILITY EXPERIENCE

One of the more complete analyses available is the General Electric study of non-nuclear power utility experience (GEAP-574). The amount of experience was one of the largest analyzed and was

sufficient to obtain statistically significant results. The data base does have the weakness that is non-nuclear. Because of the applicable general utility environment and the general agreements between nuclear and industrial data observed in the other component assessments, the G.E. results can be interpreted as being of more significant applicability. To account for the extrapolation uncertainties for nuclear applications, the results must, however, be interpreted as having large error spreads.

The G.E. basic data are summarized as follows:

Plant years of experience = 9×10^3*

Total number of failures = 399

Number of severances (ruptures) = 19

Severity fraction = $\frac{19}{399} = 0.05$

Percentage of failures occurring with leakage ~ 94%

Percentage of failures occurring without leakage ~ 6%

The 399 failures covered the range of more minor breaks to more severe ruptures. There were 19 failures of the large rupture type, which were characterized as being more complete type severances. The severity fraction was discussed earlier, and empirically is the ratio of severances to total number of failures. The percentage of failures occurring without leakage is in general agreement with the severity fraction.

The failure rate evaluations of the G.E. data are:

Total Failure Rate
(Per plant year)

$$= \frac{399}{9 \times 10^3} = 4 \times 10^{-2}$$

Severance Failure Rate
(Per plant year)

$$= \frac{19}{9 \times 10^3} = 2 \times 10^{-3}$$

Non-Severance Failure Rate
(Per plant year)

$$= \frac{(399-19)}{9 \times 10^3} \sim 4 \times 10^{-2}$$

Since the above rates are interpretable as applying to those reported for the entire plant, the large pipe rupture rate can be evaluated as:

$$\lambda(\text{LPB}) = 2 \times 10^{-3} \times .047$$

$$= 9 \times 10^{-5}/\text{plant year} .$$

The 399 failures included minimum break sizes comparable to the small rupture sizes defined in the study, and hence a corresponding small pipe rupture rate can be obtained by using the non-severance failure rate, which is essentially the total failure rate:

$$\lambda(\text{SPB}) = 4 \times 10^{-2} \times .053 = 2 \times 10^{-3}$$

6.4.4 UNITED KINGDOM DATA

The Phillips and Warwick report (AHSB(S) R162) principally analyzed pressure vessel failures; however, some piping data were included. Non-nuclear history was evaluated which covered the period from 1962 to 1967 and was comprised of a total of 132 failures occurring in roughly 100,300 plant years of experience. To better correlate with nuclear applications, system ages were restricted to be less than 30 years, had associated working pressures above 150 psi, and were built to the English Class 1 standards. Because the pipe failures reported on were not as detailed as the vessel failures and because of the extrapolation uncertainties, the results must be interpreted as having larger associated error spreads. The evaluations of the Primary Circuit Piping Failure Rate (per plant year) are:

Potentially Dangerous	Catastrophic
5×10^{-4}	2×10^{-5}

The potentially dangerous rate corresponds approximately to a range greater than minor leaks but less than complete severance. The value can thus be taken as roughly comparable to the small pipe LOCA rate. The catastrophic rate can be taken as being roughly comparable to the large LOCA rate.

*The plant years have been obtained from data and some analyses, where the plant years can be taken to be roughly equivalent to nuclear plant years.

As one other data source, the UK Systems Reliability Service, in its data evaluations, reports a rate of pipe defects to be approximately 3 in 10^7 feet of piping per year. The defect severities cover the spectrum from smaller breaks to larger ruptures. This rate is based on experience with approximately 70 conventional boiler plants operating in the 100 to 500 MW range.

If this total plant failure rate is applied as an upper bound to the large LOCA sensitive piping, then a value is obtained of:

$$\lambda \leq 3 \times 10^{-3}/\text{plant year} .$$

Because of the defect definition, the 3×10^{-3} value can also be taken as an upper bound for the small LOCA failure rate. Since the defects cover a spectrum of severities, this bound can overestimate the true LOCA failure rate by an order of magnitude. Using the same factors as previously, the associated large pipe LOCA rate or small LOCA rate can be obtained by applying the 0.05 approximate severity factor obtaining the value of:

$$\lambda(\text{LPB}) \sim 3 \times 10^{-3} \times 0.05$$

$$= 1.5 \times 10^{-4}/\text{plant year} .$$

The factor and its uncertainty can cancel any conservatism in this large pipe value.

6.4.5 OTHER REPORTED PIPE FAILURE RATES

Listed on Table III 6-10 are pipe failure rates which have been given in various published reports. The references are with regard to those given in the bibliography found in section 7 and are associated with the study's data base. The reported values are taken at face value since insufficient documentation was provided in the reports to be able to assess the relative validity of the numbers. The values are in general similar, with a few having higher deviations.

6.5 FAILURE RATES COMPARED WITH LOG NORMAL

Figures III 6-6 through III 6-9 illustrate the log-normal model distributions versus experience failure data. The log-normal distributions are those utilized in the study to predict variations in component failure data. The experience failure data consist of the raw data which were obtained from the various sources employed in the data assessments. Since the log-normal distributions utilized in the study are based on data assessment and not on simple empirical fitting, the distributions will not necessarily "best fit" the experience data (in the data assessments performed, for example, greater importance is given to nuclear and nuclear related data than to data which are not as directly applicable).

References

1. Rook, L. W., Reduction of Human Error in Industrial Production, SCTM-93-62(14), Sandia Laboratories, Albuquerque, New Mexico, 1962.

2. Swain, A. D., A Method for Performing a Human Factors Reliabiliy Analysis, Monograph SCR-685, Sandia Laboratories, Albuquerque, New Mexico, 1963.

3. Ablitt, J. F., A Quantitative Approach to the Evaluation of the Safety Function of Operators of Nuclear Reactors, AHSB(S)R-160. Authority Health and Safety Branch, United Kingdom Atomic Energy Authority, Risley, England, 1969.

4. Green, A. E., Safety Assessment of Automatic and Manual Protective Systems for Reactors, AHSB(S)R-172, Authority Health and Safety Branch, United Kingdom Atomic Energy Authority, Risley, England, 1969.

5. Kletz, T. A. and Whitaker, G. D., Human Error and Plant Operation, EDN 4099, Safety and Loss Prevention Group, Petrochemicals Division, Imperial Chemical Industries, Ltd., Billingham, England, 1973.

6. Ronan, W. W., Training for Emergency Procedures in Multiengine Aircraft, AIR-153-53-FR-44, American Institutes for Research, Pittsburgh, Penna., 1953.

7. Berkun, M. M., "Performance Decrement Under Psychological Stress", Human Factors, 1964, 6, 21-30.

8. Appley, M. H. and Trumbull, R. (eds.), Psychological Stress, Appleton-Century-Crofts, New York, 1967.

9. Harris, D. H. and Chaney, F. B., Human Factors in Quality Assurance, John Wiley and Sons, New York, 1969.

10. McCornack, R. L., Inspector Adequacy: A Study of the Literature, SCTM-53-61(14), Sandia Laboratories, Albuquerque, New Mexico, 1961.

11. Siegel, A. I. and Wolf, J. A., Man-Machine Simulation Models, John Wiley and Sons, New York, 1969.

12. Grinker, R. R. and Spiegel, J. P., Men Under Stress, McGraw Hill Book Co., 1963 (reprinted from 1945).

13. _____, Some Limitations in Using the Simple Multiplicative Model in Behavior Quantification", W. B. Askren (ed.), Symposium on Reliability of Human Performance in Work, AMRL-TR-67-88, Wright-Patterson Air Force Base, Ohio, 1967.

14. Raudenbush, M. H., "Human Engineering Factors in Control Board Design for Nuclear Power Plants", Nuclear Safety, 1973, 14, 21-26

15. MIL-H-46855A, Military Specification, Human Engineering Requirements for Military Systems, Equipment and Facilities, U.S. Dept. of Defense, Wash., D.C., 2 May 1972.

16. MIL-STD-1472A, Military Standard, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, U.S. Dept. of Defense, Wash., D.C., 15 May 1970.

17. Morgan, C. T., Cook, J. S. III, Chapanis, A. and Lund, M. W. (eds.), Human Engineering Guide to Equipment Design, McGraw Hill Book Co., New York, 1963.

18. Van Cott, H. P. and Kincade, R. G. (eds.), Human Engineering Guide to Equipment Design, (Rev. Ed.), U.S. Govt. Printing Office, Wash., D.C., 1972.

19. Woodson, W. E., and Conover, D. W., Human Engineering Guide for Equipment Designers, Univ. of California Press, Berkeley, Cal., 1964 (2nd ed.)

20. Insurance Facts (1972), (Disaster Impact Data) Insurance Information Institute, New York, New York.

21. Docket 50-289 (Aircraft Impact Data) Files, Bethesda, Maryland.

22. FAA (Air Traffic Data) Federal Aviation Administration (FAA), Dept. of Transportation, Washington, D.C.

23. D. G. Eisenhut, "General Aviation Fatal Crash Probability Distribution for Use in Nuclear Reactor Sitings", August 1972.

24. Reactor Incident File (1972) (Component Failure Data) Office or Operations Evaluation (OOE) of Regulatory Operations (RO), Atomic Energy Commission (AEC), Bethesda, Maryland.

25. Reactor Incident File (1971) (Component Failure Data) Data control of RSS, Bethesda, Maryland.

26. EEI Availability Report (Component Failure Data) Edison Electric Institute (EEI), New York, New York.

27. Systems Reliability Service, UKAEA, Office of Operations Evaluation (OOE) of Regulatory Operations (RO) are Members of Service.

28. Insurance Facts (1972), (Disaster Impact Data) Insurance Information Institute, New York, New York.

29. Docket 50-289 (Aircraft Impact Data) Files, Bethesda, Maryland.

TABLE III 6-1. GENERAL ERROR RATE ESTIMATES[a,b]

Estimated Rates	Activity
10^{-4}	Selection of a key-operated switch rather than a non-key switch (this value does not include the error of decision where the operator misinterprets situation and believes key switch is correct choice).
10^{-3}	Selection of a switch (or pair of switches) dissimilar in shape or location to the desired switch (or pair of switches), assuming no decision error. For example, operator actuates large handled switch rather than small switch.
3×10^{-3}	General human error of commission, e.g., misreading label and therefore selecting wrong switch.
10^{-2}	General human error of omission where there is no display in the control room of the status of the item omitted, e.g., failure to return manually operated test valve to proper configuration after maintenance.
3×10^{-3}	Errors of omission, where the items being omitted are embedded in a procedure rather than at the end as above.
3×10^{-2}	Simple arithmetic errors with self-checking but without repeating the calculation by re-doing it on another piece of paper.
1/x	Given that an operator is reaching for an incorrect switch (or pair of switches), he selects a particular similar appearing switch (or pair of switches), where x = the number of incorrect switches (or pair of switches) adjacent to the desired switch (or pair of switches). The 1/x applies up to 5 or 6 items. After that point the error rate would be lower because the operator would take more time to search. With up to 5 or 6 items he doesn't expect to be wrong and therefore is more likely to do less deliberate searching.
10^{-1}	Given that an operator is reaching for a wrong motor operated valve MOV switch (or pair of switches), he fails to note from the indicator lamps that the MOV(s) is (are) already in the desired state and merely changes the status of the MOV(s) without recognizing he had selected the wrong switch(es).
~1.0	Same as above, except that the state(s) of the incorrect switch(es) is (are) <u>not</u> the desired state.
~1.0	If an operator fails to operate correctly one of two closely coupled valves or switches in a procedural step, he also fails to correctly operate the other valve.
10^{-1}	Monitor or inspector fails to recognize initial error by operator. Note: With continuing feedback of the error on the annunciator panel, this high error rate would not apply.
10^{-1}	Personnel on different work shift fail to check condition of hardware unless required by check list or written directive.
5×10^{-1}	Monitor fails to detect undesired position of valves, etc., during general walk-around inspections, assuming no check list is used.
.2 - 3	General error rate given very high stress levels where dangerous activities are occurring rapidly.

TABLE III 6-1 . (Continued)

Estimated Rates	Activity
$2^{(n-1)}x$	Given severe time stress, as in trying to compensate for an error made in an emergency situation, the initial error rate, x, for an activity doubles for each attempt, n, after a previous incorrect attempt, until the limiting condition of an error rate of 1.0 is reached or until time runs out. This limiting condition corresponds to an individual's becoming completely disorganized or ineffective.
~1.0	Operator fails to act correctly in the first 60 seconds after the onset of an extremely high stress condition, e.g., a large LOCA.
9×10^{-1}	Operator fails to act correctly after the first 5 minutes after the onset of an extremely high stress condition.
10^{-1}	Operator fails to act correctly after the first 30 minutes in an extreme stress condition.
10^{-2}	Operator fails to act correctly after the first several hours in a high stress condition.
x	After 7 days after a large LOCA, there is a complete recovery to the normal error rate, x, for any task.

(a) Modification of these underlying (basic) probabilities were made on the basis of individual factors pertaining to the tasks evaluated.

(b) Unless otherwise indicated, estimates of error rates assume no undue time pressures or stresses related to accidents.

TABLE III 6-2 AIRCRAFT CRASH PROBABILITIES

Distance From Airport, miles	Probability of a Fatal Crash per Mile^2 Per Aircraft Movement
0 - 1	84×10^{-8}
1 - 2	15×10^{-8}
2 - 3	6.2×10^{-8}
3 - 4	3.8×10^{-8}
4 - 5	1.2×10^{-8}

TABLE III 6-3 COMPARISON OF PROBABILITY OF AN AIRCRAFT CRASH FOR VARIOUS TYPES OF AIRCRAFT

Distance From End Of Runway, (mile)	Probability ($x10^8$) of a Fatal Crash Per Square Mile per Aircraft Movement		
	U.S. Air Carrier	USN/USMC	USAF
0 - 1	16.7	8.3	5.7
1 - 2	4.0	1.1	2.3
2 - 3	0.96	0.33	1.1
3 - 4	0.68	0.31	0 42
4 - 5	0.27	0.20	0.40
5 - 6	0 0[a]	NA[b]	NA[b]
6 - 7	0.0	NA	NA
7 - 8	0.0	NA	NA
8 - 9	0.14	NA	NA
9 - 10	0.12	NA	NA

(a) No crashes occurred at these distances within a 60° flight path.

(b) Data not available.

TABLE III 6-4 CRASH PROBABILITIES AT VARIOUS SITES

	Three Mile Island (2 Units)	Shoreham (1 Unit)	Rome Point (2 Units)	Surry Units 3-4 (2 Units)
Usage (movements year)				
Air Carriers	80,000[a]	--	3,000	40,000
Navy	--	8,000	97,000[c]	40,000
Miscellaneous	--	3,000[b]	--	--
Location (plant-airport distance in miles)	2.5	4.5	3.5	5
Target Area (used in probability analysis)	0.02 mi^2	0 01 mi^2	0.02 mi^2	.01 mi^2[d]
Probability of a potentially damaging crash (per year)	5×10^{-7}	2×10^{-7}	4×10^{-7}	1×10^{-6}

(a) The facility is designed to withstand the crash of all but 2,400 of these movements.

(b) Air-carrier statistics were used for these movements.

(c) The facility is designed to withstand the crash of all of these 97,000 movements.

(d) For small aircraft, area used was 0.005 mi^2.

TABLE III 6-5 SUMMARY OF TRANSMISSION LINE OUTAGES (BASED ON BONNEVILLE POWER ADMINISTRATION DATA--1970 STATISTICS)

Cause	Transmission Line Outages & Durations[a]														
	500 kV			345 & 287 kV			230 kV			138 & 115 kV			Total		
	No	Hr	Min	No	Hr	Min	No	Hr	Min	No	Hr	Min	No	Hr	Min
1. Tree in line	0	0	0	0	0	0	2	7	9	7	25	27	9	32	36
2. Lightning	9	1	28	4	0	38	87	27	8	71	71	46	171	101	0
3. Storm	0	0	0	0	0	0	0	0	0	4	209	57	4	209	57
4. Snow, Frost or Ice	1	0	8	0	0	0	10	29	58	23	192	23	34	222	29
5. Living Creature	0	0	0	0	0	0	0	0	0	3	0	6	3	0	6
6. Contamination	0	0	0	0	0	0	0	0	0	3	0	28	3	0	28
7. Fire	0	0	0	0	0	0	2	23	24	1	1	7	3	24	31
8. Line Material Failure	1	0	18	1	53	25	1	152	26	4	64	33	7	270	42
9. Terminal Equipment Failure	6	52	2	2	5	7	7	5	19	12	8	23	27	70	51
10. Overload	3	0	33	0	0	0	2	0	4	0	0	0	5	0	37
11. Improper Relaying	6	0	40	0	0	0	2	4	6	1	0	0	9	4	46
12. Accidental Tripping	8	9	43	5	0	14	14	3	28	4	0	25	31	13	50
13. Improper Switching	1	0	18	1	0	0	4	0	11	5	0	41	11	1	10
14. Malicious Damage	1	0	7	0	0	0	1	6	19	12	75	35	14	82	1
15. Accidental Damage	0	0	0	1	0	1	3	0	11	2	0	0	6	0	12
16 Supervisory Misoperation	0	0	0	0	0	0	0	0	0	1	0	49	1	0	49
17. Unknown	26	5	40	3	0	1	30	10	46	35	10	42	94	27	9
TOTAL	62	70	57	17	59	26	165	270	29	188	662	22	432	1063	14
MILES OF LINE	1707			797			4685			3836			11,025		

(a) In each case, the number of incidents is given together with the total time for all of those incidents.

TABLE III 6-6 SUMMARY OF TRANSMISSION LINE OUTAGES (BASED ON BONNEVILLE POWER ADMINISTRATION DATA--1971 STATISTICS)

Cause	Transmission Line Outages & Durations														
	500 kV			345 & 287 kV			230 kV			138 & 115 kV			Total		
	No	Hr	Min	No	Hr	Min	No	Hr	Min	No	Hr	Min	No	Hr	Min
1. Tree in line	0	0	0	0	0	0	0	0	0	16	176	13	16	176	13
2. Lightning	11	0	56	7	0	8	83	12	13	69	30	13	170	43	30
3. Storm	0	0	0	0	0	0	4	11	29	12	41	6	16	52	35
4. Snow, Frost or Ice	0	0	0	1	140	55	1	0	0	19	0	16	21	141	11
5. Living Creature	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
6. Contamination	5	0	20	0	0	0	4	2	10	0	0	0	9	2	30
7. Fire	0	0	0	0	0	0	3	122	57	3	28	22	6	151	19
8. Line Material Failure	1	7	2	0	0	0	2	18	26	10	32	30	13	57	58
9. Terminal Equipment Failure	6	78	56	1	0	22	15	7	11	4	2	19	26	88	48
10. Overload	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11. Improper Relaying	2	1	25	0	0	0	2	0	4	0	0	0	4	1	29
12. Accidental Tripping	9	1	14	0	0	0	10	1	11	8	1	33	27	3	58
13. Improper Switching	0	0	0	0	0	0	2	0	0	2	0	2	4	0	2
14. Malicious Damage	0	0	0	0	0	0	1	5	59	3	19	44	4	25	43
15. Accidental Damage	2	0	44	3	9	18	1	0	0	4	9	4	10	19	06
16. Supervisory Misoperation	0	0	0	0	0	0	1	0	10	3	13	47	4	13	57
17. Unknown	21	3	15	2	5	36	26	21	32	35	0	45	84	31	8
TOTAL	58	93	52	14	156	19	155	203	22	188	355	54	415	809	27
MILES OF LINE	1810			797			4836			3669			11,112		

TABLE III 6-7 SUMMARY OF TRANSMISSION LINE OUTAGES (BASED ON BONNEVILLE POWER ADMINISTRATION DATA--1972 STATISTICS)

Cause	Transmission Line Outages & Durations														
	500 kV			345 & 287 kV			230 kV			138 & 115 kV			Total		
	No	Hr	Min	No	Hr	Min	No	Hr	Min	No	Hr	Min	No	Hr	Min
1. Tree in line	0			0			4	6	10	18	145	16	22	151	26
2. Lightning	49	2	29	22		25	194	22	8	98	3	37	363	28	39
3. Storm	17	2	13	5	10	25	13	0	13	27	44	53	62	57	44
4. Snow, Frost or Ice	5	5	22	1	3	9	1	0	0	7	6	52	14	15	23
5. Living Creature	0	0	0	0	0	0	0	0	0	2	1	58	2	1	58
6. Contamination	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0
7. Fire	0	0	0	0	0	0	1	5	49	0	0	0	1	5	49
8. Line Material Failure	4	22	11	0	0	0	0	0	0	3	40	28	7	62	39
9. Terminal Equipment Failure	11	64	45	0	0	0	17	328	42	10	1	46	38	395	13
10. Overload	4	1	14	0	0	0	0	0	0	1	1	15	5	2	29
11. Improper Relaying	6	1	46	1	0	0	8	0	57	6	0	26	21	3	9
12. Accidental Tripping	11	2	8	1	0	0	18	1	30	7	0	35	37	4	13
13. Improper Switching	2	0	16	0	0	0	3	0	14	3	0	7	8	0	37
14. Malicious Damage	0	0	0	0	0	0	2	15	33	9	76	11	11	91	44
15. Accidental Damage	0	0	0	0	0	0	2	12	26	38	16	23	40	28	49
16. Supervisory Misoperation	0	0	0	0	0	0	2	0	51	2	1	4	4	1	55
17. Unknown	35	45	8	5	0	15	19	2	2	44	2	16	103	49	41
TOTAL	144	147	32	35	14	14	284	396	35	276	343	7	739	901	28
MILES OF LINE		1931			797			4601			3676			11,005	

TABLE III 6-8 PROBABILITY OF TOTAL LOSS OF ELECTRIC POWER AFTER A LOCA

Time after LOCA	Q_{med}	90 percent Probability Bounds[a] Upper	Lower
1 hour	2.0×10^{-7}	2.0×10^{-6}	2.0×10^{-8}
24 hours	5.2×10^{-6}	5.0×10^{-5}	5.0×10^{-7}
4 months	7.5×10^{-5}	7.0×10^{-4}	7.0×10^{-6}
9 months	7.6×10^{-5}	8.0×10^{-4}	8.0×10^{-6}

(a) Assessed range.

TABLE III 6-9 PIPE FAILURE ASSESSED VALUES

Pipe Rupture Size (Inches)	LOCA Initiating Rupture Rates (Per Plant Per Year)	
	90% Range	Median
1/2 - 2	$1x10^{-4}$ - $1x10^{-2}$	$1x10^{-3}$
2 - 6	$3x10^{-5}$ - $3x10^{-3}$	$3x10^{-4}$
> 6	$1x10^{-5}$ - $1x10^{-3}$	$1x10^{-4}$

TABLE III 6-10 REPORTED PIPE FAILURE RATES

1. Green and Bourne:
   "Probability of Large Scale Rupture of Primary Coolant System"
   (1968) $\lambda = 2 \times 10^{-3}$ to 3×10^{-6}/plant year

2. Salvatory:
   "Catastrophic Rupture of Primary System Pipes"
   (1970) $\lambda = 1 \times 10^{-4}$/plant year

3. Erdmann:
   "Pipe Rupture"
   (1973) $\lambda = 1.5 \times 10^{-6}$/section year
   (corresponding to roughly $\lambda = 10^{-4}$ to 10^{-2} per plant year)

4. Otway:
   "Pessimistic Probability for Catastrophic Failure of Primary System of PWR"
   $\lambda = 1.7 \times 10^{-7}$/plant year

5. General Electric Report:
   "Total Probability of Severance Anywhere in Primary System Piping"
   (1970)
   without ultrasonic testing: $\lambda = 1 \times 10^{-3}$/plant year
   with ultrasonic testing: $\lambda = 5 \times 10^{-4}$/plant year

6. Wells-Knecht:
   "Failure Rate for Rupture of Primary Coolant System Piping"
   (1965) $\lambda = 1 \times 10^{-7}$/plant year

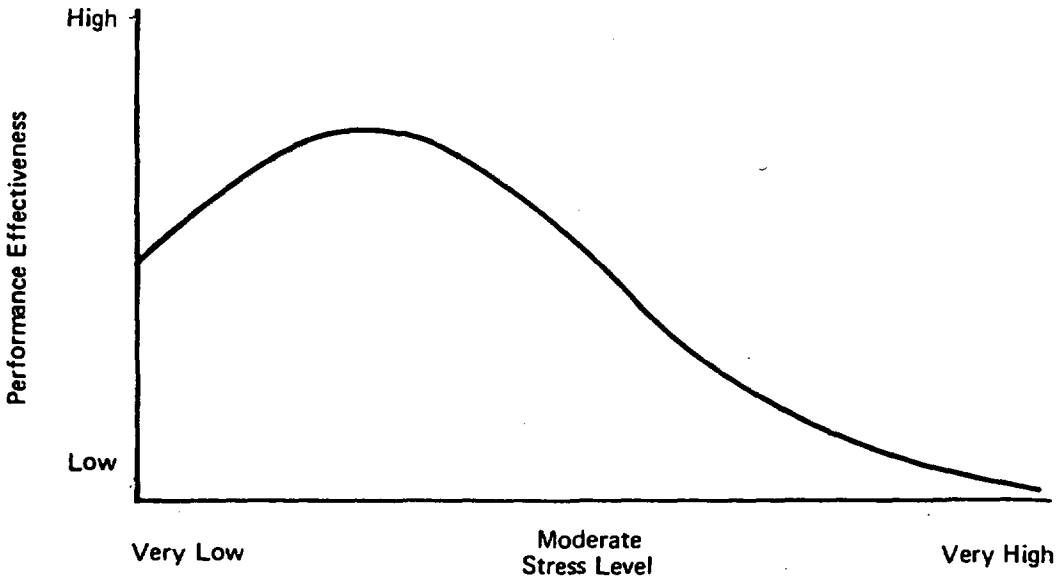


FIGURE III 6-1 Hypothetical Relationship between Performance and Stress

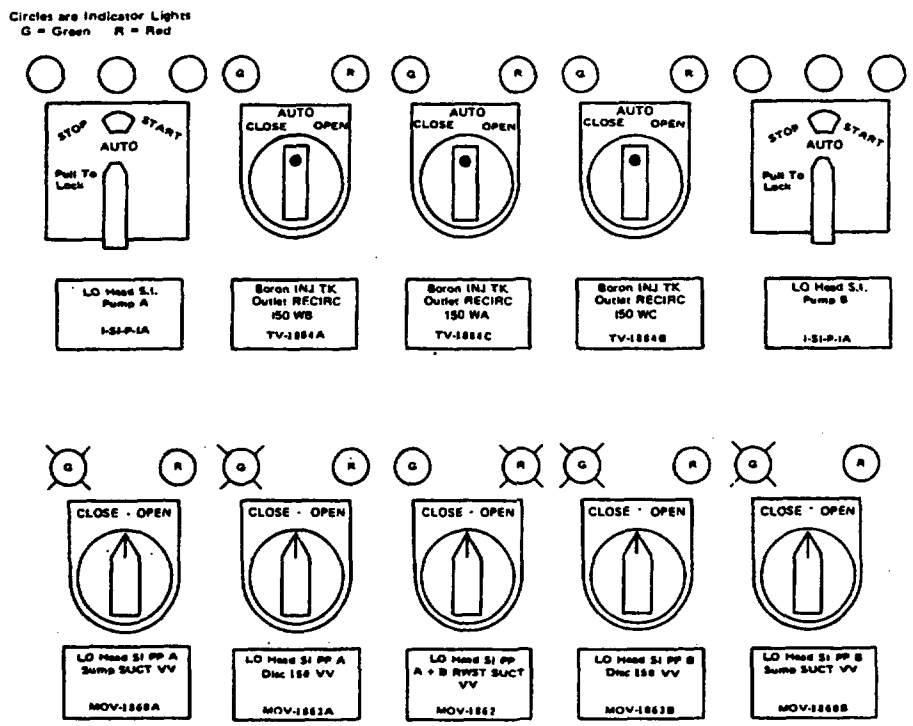


FIGURE III 6-2 Motor Operated Valve (MOV) Switches on Control Panel

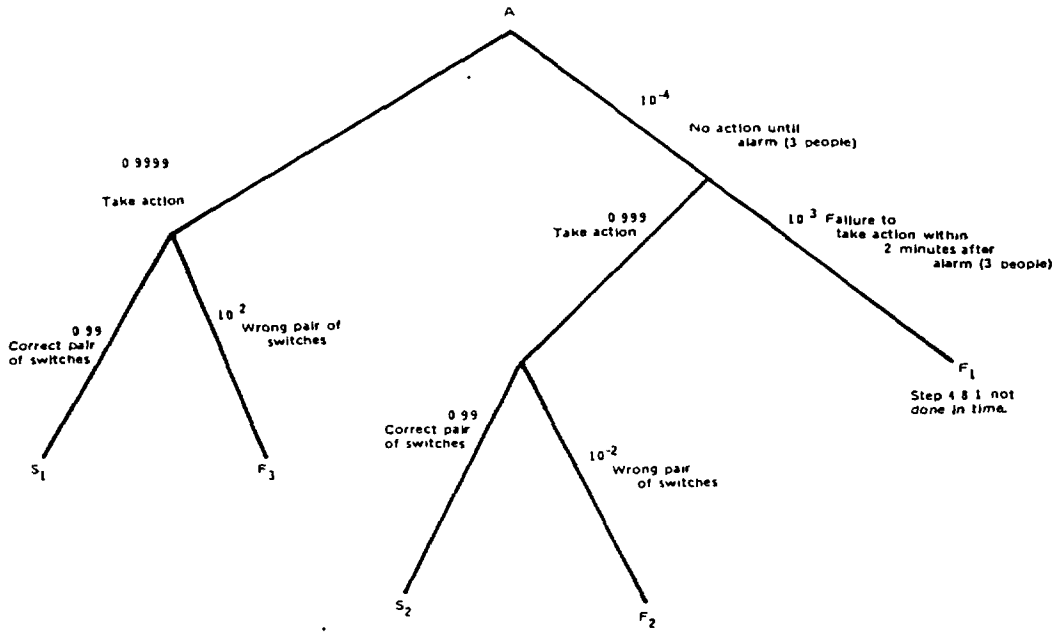


FIGURE III 6-3 Probability Tree Diagram for Step 4.8.1

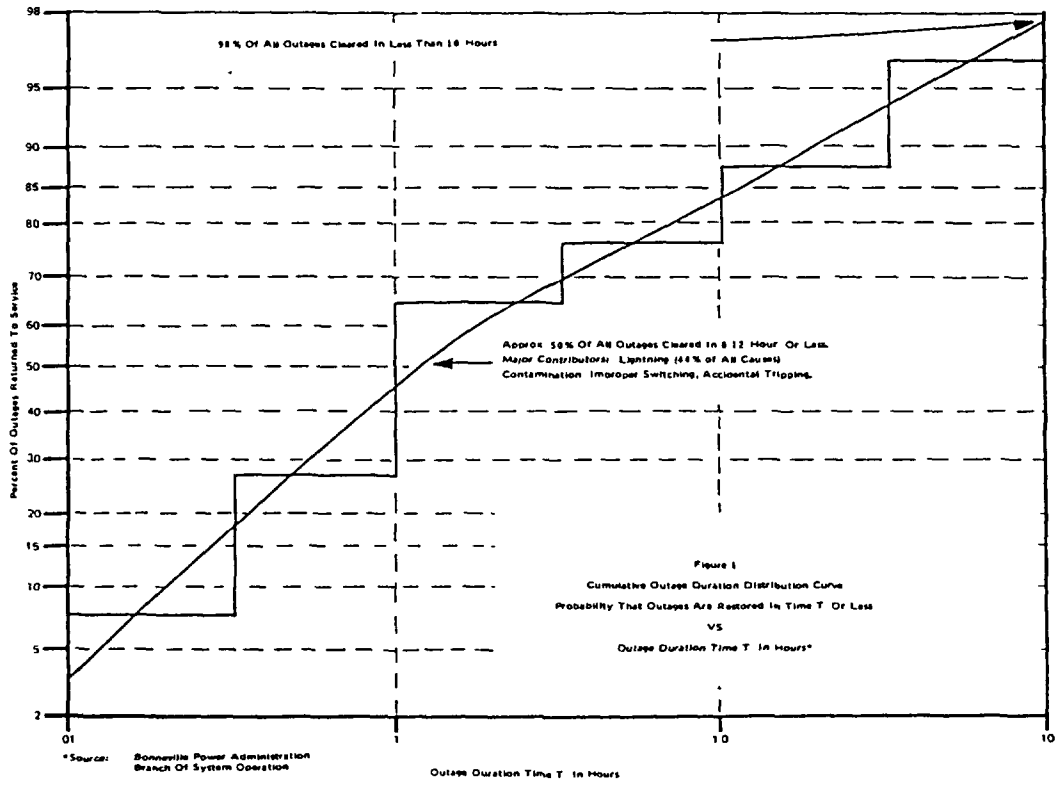


FIGURE III 6-4 Cumulative Outage Duration Distribution Curve

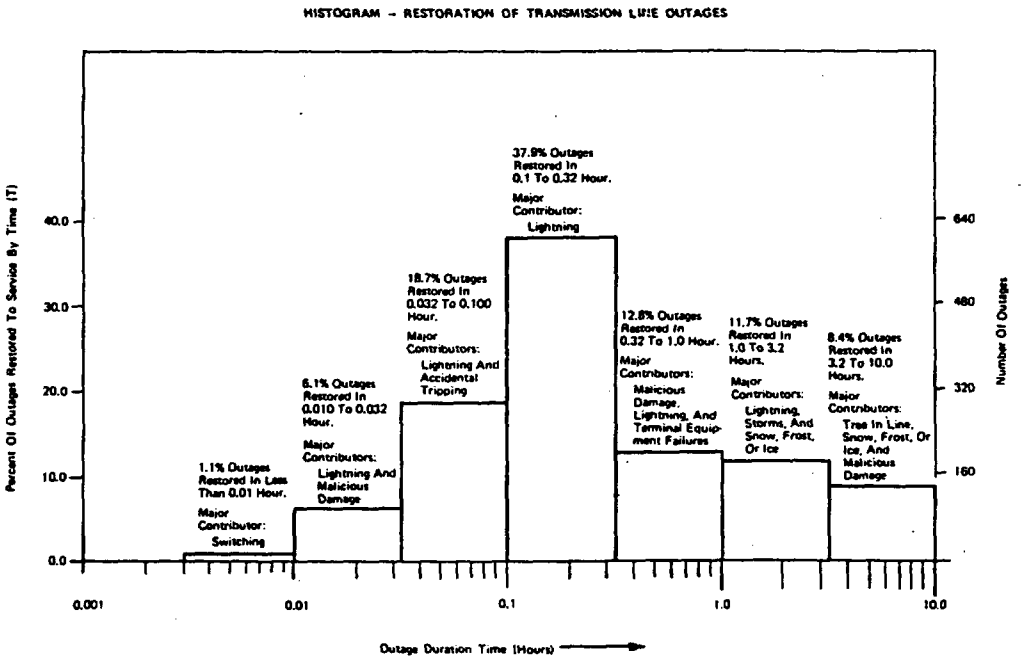


FIGURE III 6-5 Histogram - Restoration of Transmission Line Outages

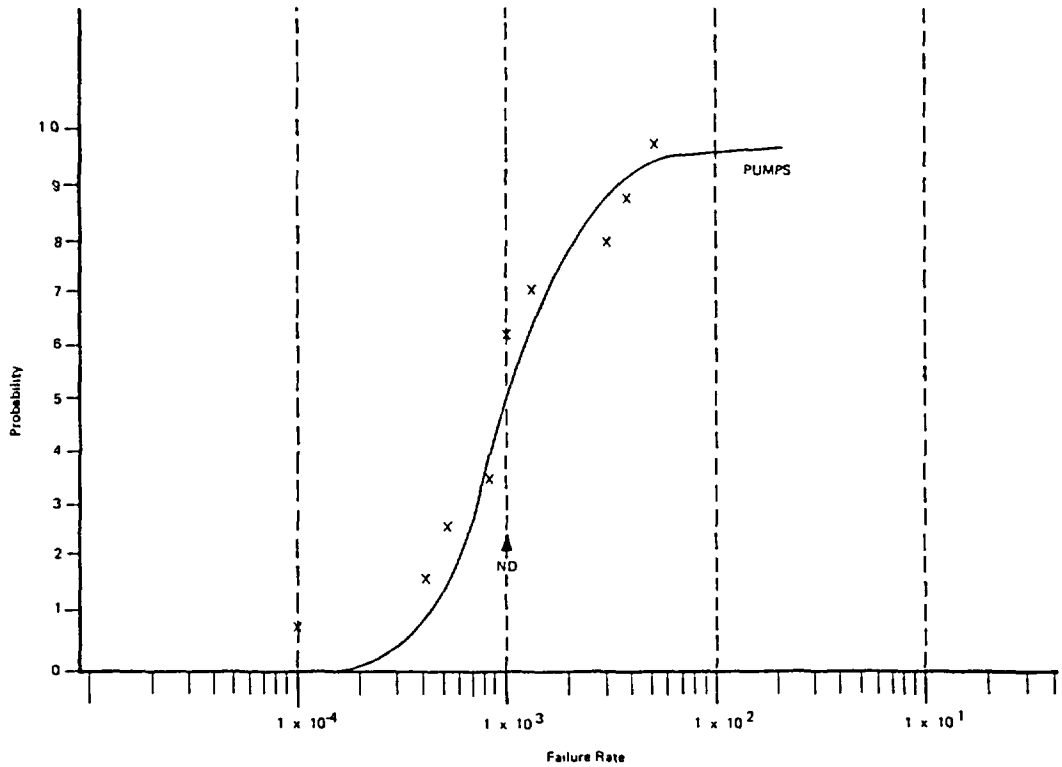


FIGURE III 6-6 Log-Normal Distribution - Pumps

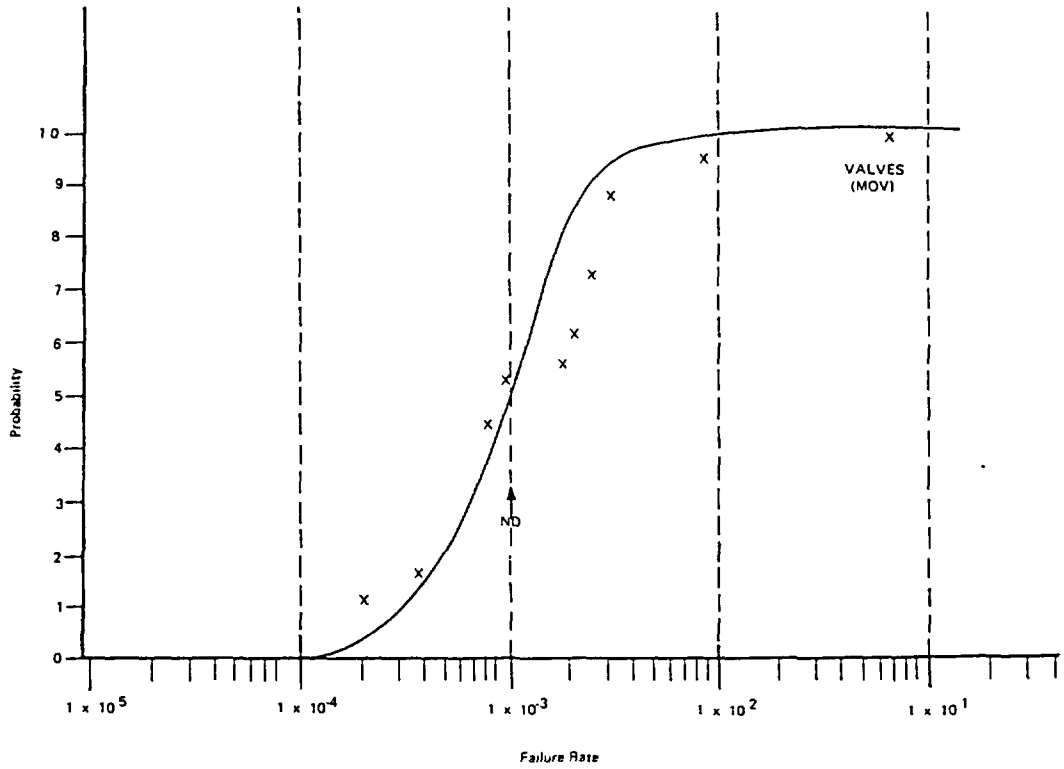


FIGURE III 6-7 Log-Normal Distribution - Valves

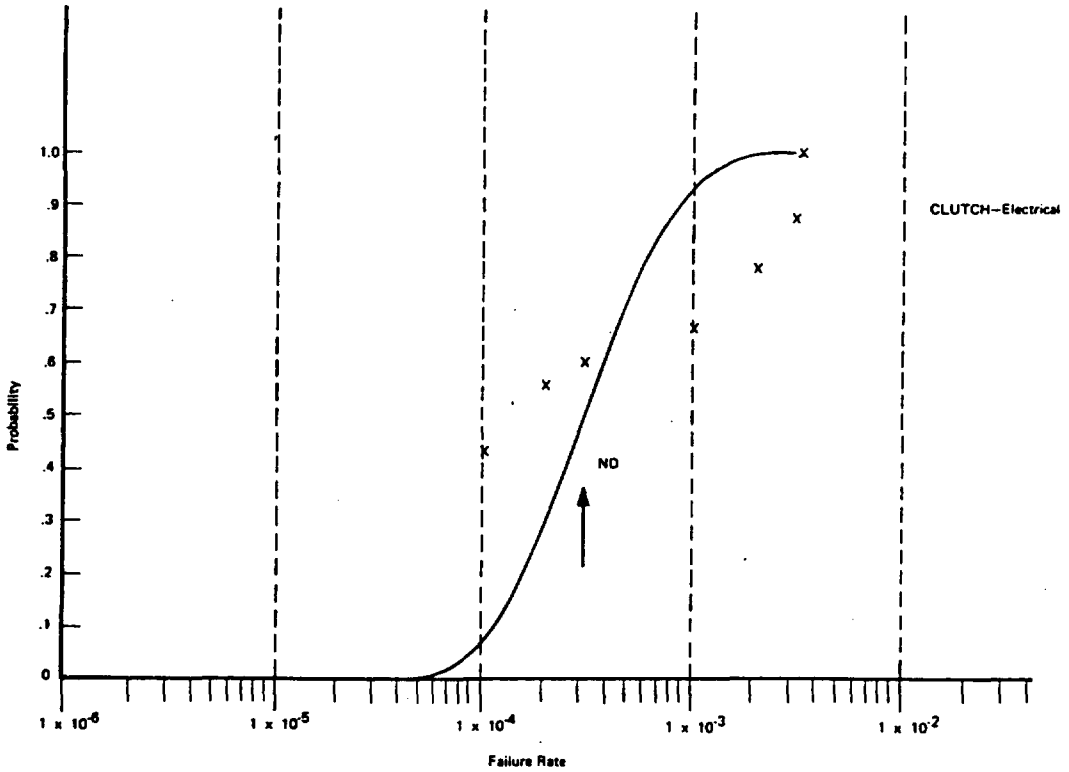


FIGURE III 6-8 Log-Normal Distribution - Clutch - Electrical

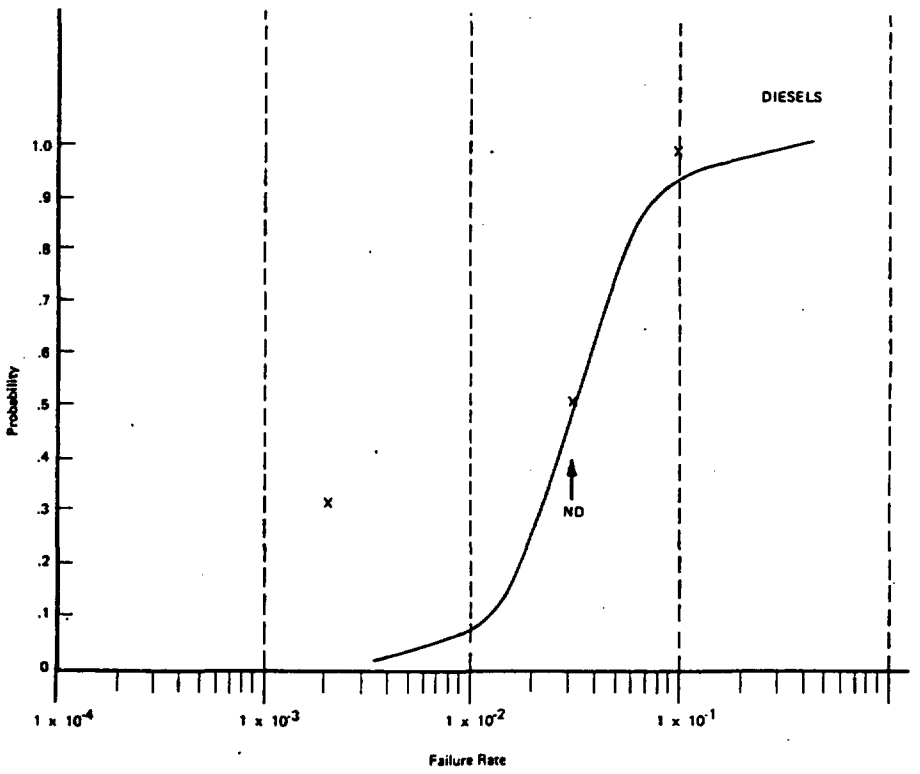


FIGURE III 6-9 Log-Normal Distribution - Diesels

Fig. III 6-6 — Fig. III 6-9

Section 7
References

7.1 DISCUSSION OF REFERENCES

In addition to the Nuclear Operating experiences (Refs. 1, 2 and 3,) approximately 50 other sources of failure rates and failure data were reviewed in support of the estimates used in this analysis. These sources can be broadly grouped into two categories: (1) general reliability data sources and (2) special sources.

7.2 GENERAL SOURCES

The general sources consist primarily of the United Kingdom Systems Reliability Service, FARADA, AVCO, LMEC, Collins and Pomeroy and Holmes and Narver. These sources provide failure data on a spectrum of hardware and failure modes from a variety of applications including nuclear and non-nuclear utilities, test and research reactors and military and NASA components.

7.3 SPECIAL SOURCES

The other sources are described as special in that they generally contain information on particular hardware failure modes or operating conditions. For example, References 10, 12, 13, 14, 15, 16, 17, 18 and 20 involve pipe and pipe hardware failures. References 23, 24, 25, 26 and 27 refer to aircraft accidents, earthquakes and other background phenomena. References 34 through 52 contain analyses of particular hardware and systems in nuclear and non-nuclear utilities and chemical industry applications.

It should be noted that these references do not represent 50 independent sources. Some refer to and use data from other references by updating, the data to reflect current experiences and interests. The references, therefore, represent a broadly based amalgamation of experience, operation conditions, and use applications.

	Reference	Contact, Service Office or Originator	Contact, Report or Source Date	Report, Listing Source or Content
1.	Reactor Incident File (1972) (Component Failure Data)	Office or Operations Evaluation (OOE) of Regulatory Operations (RO), Atomic Energy Commission (AEC), Bethesda, Maryland.	1/1/72 to 12/31/72	Contains approximately 30% unusual occurrences at nuclear facilities and 90% of reportable abnormal occurrences observed in the year of 1972.
2.	Reactor Incident File (1971) (Component Failure Data)	Data control of RSS, Bethesda, Maryland.	9/4/73	Contains approximately one quarter of 1971 unusual and abnormal occurrences observed from the files of OOE.
3.	EEI Availability Report (Component Failure Data)	Edison Electric Institute (EEI), New York, New York.	8/16/73 & 10/12/73	Contains 66 unit years of fossil and nuclear power plants component availability and outage statistics of contributing facilities.
4.	Systems Reliability Service, UKAEA	Office of Operations Evaluation (OOE) of Regulatory Operations (RO) are Members of Service.	All Service Publications plus Special Requests 9/12/73.	Contains Failure Rate Assessments derived. UK and other available European sources.

	Reference	Contact, Service Office or Originator	Contact, Report or Source Date	Report, Listing Source or Content
5.	FARADA	Converged Failure Rate Data Handbooks, published by Fleet Missile Systems Analysis and Evaluation Group Annex, NWS, Sea Beach, Corona, Calif.	All current issues.	Contains Failure Rate Assessments derived from Army, Navy, Air Force, and NASA sources.
6.	AVCO	Reliability Engineering Data Services Failure Rates. AVCO Corp.	1962	Contains Failure Rate Assessments for primarily military quality hardware.
7.	LMEC	Failure Data Handbook For Nuclear Power Facilities, Liquid Metal Engineering Center.	1969	Compilation of failure rates derived from test and research reactor operating experiences.
8.	Collins & Pomeroy	Environmental Reports, Directorate of Licensing, Division of Compliance, Regulatory, AEC.	11/1/71	Operating experience and related data from literature in support of occurrence rates to be assumed for further interim guidance on accident evaluations.
9.	Holmes & Narver	Collection of reliability data at nuclear power plants, Holmes & Narver, Inc.	1968	Contains failure rate data gathered from operating experience, one plant--4 months.
10.	Chemical Abstracts (Piping Failure Data)	AEC Headquarters Library, Germantown, Maryland.	9/24/73	Bibliography listing of metallurgical and piping analysis reports (65) of industrial conduit systems.
11.	The Chemical Engineer	The Institution of Chemical Engineers, 16 Redgrave, London S.W.1	1971	Contains data on reliability of instruments in the chemical plant environment.
12.	NASA Literature Search (Piping Failure Data)	Information Tisco Inc., NASA Scientific and Technical Information Facility, College Park, Maryland.	9/12/73	Listing of steam pipe failure reports (393) for normal and limited distribution of industrial steam systems.
13.	AEC RECON (Piping Failure Data)	AEC Headquarters Library, Germantown, Maryland.	9/10/73	Listing of Nuclear Science Abstracts search on pipe rupture and pressure vessel analysis of primary steam systems.
14.	DOT Pipeline Safety (Pipeline Leak Summary)	Office of Pipeline Safety, Department of Transportation (DOT), Office of the Secretary, Washington, D.C.	10/10/73	1971 and 1972 gas pipe line leak and rupture history of transmission and distribution systems throughout the United States.

	Reference	Contact, Service Office or Originator	Contact, Report or Source Date	Report, Listing Source or Content
15.	NSIC Literature Search (Piping Failures)	Nuclear Safety Information Center (NSIC) of the AEC, Oak Ridge, Tennessee.	9/13/73	Listing of references of piping failures (317) in industrial uses of atomic power.
16.	GIDEP "ALERT" (Manufacturing Defects)	National Technical Information Service (NTIS) U.S. Department of Commerce, Springfield, Virginia.	9/3/73	Parts, materials, and processes experience summary of NASA and Government-Industry Data Exchange Program (GIDEP) reports.
17.	NAVSHIPS Report (Main Steam Piping Data)	Maintenance Support Office, Naval Ship Systems Command, Department of the Navy, Arlington, Virginia.	10/3/73	Printouts contain maintenance data covering main steam piping on nuclear submarines and surface ships for a three year period ('70, '71, and '72).
18.	DDC Literature Search (Steam & Water Pipe Failures)	Defense Documentation Center (DDC), Defense Supply Agency, Alexandria, Virginia.	9/12/73	Bibliography of piping problems and simulated failures throughout the military and industrial world. (53 itemized descriptions).
19.	DDC Literature Search (Manufacturing Defects)	Defense Documentation Center (DDC), Defense Supply Agency, Alexandria, Virginia.	8/23/73	Bibliography on probabilities of manufacturing errors from the standpoint of design evaluations (147 items).
20.	GEAP (Piping Failure Data)	General Electric Company, Atomic Power Department, San Jose, California.	1964 thru 1972	Periodic reports (series 10207 of the Reactor Primary Coolant System Pipe Rupture Study summarizing failure mechanisims and probabilities.
21.	Nuclear Science Abstracts (Containment Breaches)	Technical Information Center (TIC) of the U.S. Atomic Energy Commission, Oak Ridge, Tennessee.	1967 thru 1972	Subject index for nuclear scientific reports over a six year period. Reference book.
22.	NSIC Literature Search (Special Common Mode Failures)	Nuclear Safety Information Center (NSIC) of the U.S. Atomic Energy Commission, Oak Ridge, Tennessee.	8/2/72	A ten year literature search for five categories of qualitative reports and bibliographies.
23.	Engineering Index (Environmental Factors)	AEC Headquarters Library, Germantown, Maryland.	8/17/73	A search for quantitative reports on the earthquakes electrical fires and airplane crashes.
24.	Geologic Literature Search (Disaster Impact Data)	American Geologic Institute, Washington, D.C.	8/17/73	A listing of topics (220) associated with earthquake predictions from the standpoint of geologic effects.

	Reference	Contact, Service Office or Originator	Contact Report or Source Date	Report, Listing Source or Content
25.	DDC Literature Search (Disaster Impact Data)	Defense Documentation Center (DDC), Defense Supply Agency, Alexandria, Virginia.	8/21/73	Bibliography on unusual natural occurrences (192).
26.	Insurance Facts (1972) (Disaster Impact Data)	Insurance Information Institute, New York, New York.	8/20/73	A yearbook of property and liability insurance facts of losses as reported by U.S. companies.
27.	RESPONSA (Seismic Effect Data)	Selected Nuclear Science Abstracts (RESPONSA), AEC Headquarters Library, Germantown, Maryland.	8/15/73	Listing of seismic topics (245) for reactor siting and nuclear application: includes docket material.
28.	RESPONSA (ECCS Analysis Data)	Selected Nuclear Science Abstracts (RESPONSA), AEC Headquarters Library, Germantown, Maryland.	8/1/73	Listing of Emergency Core Cooling System (ECCS) topics (approx. 928) and associated analysis.
29.	RESPONSA (Parts & Materials Data)	Selected Nuclear Science Abstracts (RESPONSA), AEC Headquarters Library, Germantown, Maryland.	8/24/73	Listing of topics (approx. 936) on fractures of reactor parts and materials with emphasis on steel and alloys.
30.	NASA Literature Search (Disaster)	Information Tisco Inc., Scientific and Technical Information Facility, College Park, Maryland.	8/17/73	Listing of disaster prediction or forecasting reports (608) on meteorological and climatological measurements.
31.	NASA Literature Search (Manufacturing Defects)	Information Tisco Inc., NASA Scientific and Technical Information Facility, College Park, Maryland.	8/23/73	Quality control in manufacture of machinery or power generating equipment a brief survey.
32.	Docket 50-289 (Aircraft Impact Data)	Files, Bethesda, Maryland.	8/28/73	Three Mile Island Unit 1 (Metropolitan Edison Co. of Pennsylvania) report, Summary of Aircraft Impact Design.
33.	FAA (Air Traffic Data)	Federal Aviation Administration (FAA), Dept. of Transportation, Washington, D.C.	March 1972	En Route IFR Air Traffic Survey Peak-Day FY 1971, authored by the FAA Statistical Division.

34. Letter from W. F. Shopsky to D. F. Paddleford dated October 20, 1972.

35. A. J. Bourne, "Reliability Assessment of Technological Systems," Report, Systems Reliability Service, UKAEA, October 1971.

36. K. H. Lindackers, W. Stoebel, Part I, O. A. Kellerman, W. Ullrich, Part II: Probability Analysis Applied to LWR's, Institute of Reactor Safety, W. Germany, Paper 9.

37. F. M. Davies, "A Worked Example on the Use of Reliability Analysis Techniques - Decay Heat Removal", Lecture No. 58 Reactor Assessment, Section I, Safety and Reliability Directorate, Risley, U.K.

38. "Meeting of Specialists on the Reliability of Electrical Supply Systems and Related Electric-Mechanical Components for Nuclear Reactor Safety", European Nuclear Energy Agency Committee on Reactor Safety Technology, Session I, Ispra, Italy, (June 27-28, 1968).

39. M. C. Pugh, "Probability Approach to Safety Analysis", United Kingdom Atomic Energy Authority, 1969.

40. R. M. Stewart, G. Hensley, "High Integrity Protective Systems on Hazardous Chemical Plants", European Nuclear Energy Agency Committee on Reactor Safety Technology, Munich (May 26-28, 1971).

41. J. C. Moore, "Research Reactor Fault Analysis", Parts I and II, Nuclear Engineering (March, June 1966).

42. "IEEE Transactions on Nuclear Science", Volume NS-18, February 1971.

    a. B. M. Tashjian, "Sensitivity Analysis of a Two-out-of-Four Coincident Logic Reactor Protective System" pg. 455.

    b. R. Salvatori, "Systematic Approach to Safety Design and Evaluation, pg. 495.

43. A. J. Bourne, G. Hensley, A. R. Eames, A. Aitken, "Reliability Assessment of the S.G.H.W.R. Liquid Shutdown System", AHSB(S)R 144 (March 1968).

44. H. J. Otway, R. K. Lohrding, M. E. Battat, "A Risk Estimate for an Urban-Sited Reactor", Nuclear Technology, Vol. 12 October 1971.

45. F. R. Farmer, "Siting Criteria - A New Approach", United Kingdom Atmoic Energy Authority, Risley, Warrington, Lancs, U.K.

46. J. R. Beattie, G. D. Bell, J. E. Edwards, "Methods for the Evaluation of Risk", AHSB(S)R 159 UKAEA, (1968).

47. G. D. Bell, "Risk Evaluation for Any Curie Release Spectrum and Any Dose Rise Relationship", AHSB(S)R 192, UKAEA, (1971).

48. "Fault Tree Analysis, SPERT IV Scram System" INC Work Request No. N-42128.

49. W. L. Headington, M. E. Stewart, J. O. Zane, "Fault Tree Analysis of the PBF Transient Rod Drive System", IDO-17272 (November 1968).

50. Gulf Electronics Systems, Nuclear Instrumentation Specifications.

51. "Proceedings of the Meeting of Specialists on the Reliability of Mechanical Components and Systems for Nuclear Reactor Safety," RISO Report No. 214, Establishment (February 1970).

    a. S. Antocisco, G. Tenoglia, A. Valeri, "A Theoretical Reliability Assessment of a Fire Protection System", pg. 22.

    b. W. Bastl, H. Gieseler, H. A. Maurer, U. Hennings, "The Reliability of Emergency Core Cooling Systems of Light Water Nuclear Plants", pg. 91.

    c. H. Huppman, "Frequency and Causes of Failure to Components of Large Steam Turbines", pg. 171.

    d. U. Hennings, "Auslegung and Anordnung Einer Reaktor-Beschickungsan-lage Auggrund von Zwerlassigngeitsbetrachtungen" pg. 213.

    e. G. Mieze, "Analysis of a German Pressure Vessel and Boiler Drum Statistics", pg. 301.

f. G. A. G. Phillips, R. G. Warwick, "A Survey of Pressure Vessels Built to a High Standard of Construction", pg. 323.

g. J. Ehrentreich, H. Maurer, "Reliability Considerations for Mechanical Components of Control Rod Drive Systems of Gas Cooled Power Reactors Operated in the European Community", pg. 481.

52. NRTS National Reactor Testing Station, Ihaho: Failure History 1968-1972, B. A. Thomas ETAL.

53. D. G. Eisenhut, "General Avaiation Fatal Crash Probability Distribution for Use in Nuclear Reactor Sitings", August 1972.

54. Ablitt, J. F., A Quantitative Approach to the Evaluation of the Safety Function of Operators of Nuclear Reactors, AHSB(S)R-160, Authority Health and Safety Branch, United Kingdom Atomic Energy Authority, Risley, England, 1969.

55. Appley, M. H. and Trumbull, R. (eds.), Psychological Stress, Appleton-Century-Crofts, New York, 1967.

56. Berkun, M. M., "Performance Decrement Under Psychological Stress", Human Factors, 1964, 6, 21-30.

57. Green, A. E., Safety Assessment of Automatic and Manual Protective Systems for Reactors, AHSB(S)R-172, Authority Health and Safety Branch, United Kingdom Atomic Energy Authority, Risley, England, 1969.

58. Grinker, R. R. and Spiegel, J. P., Men Under Stress, McGraw Hill Book Co., 1963 (reprinted from 1945).

59. Harris, D. H. and Chaney, F. B., Human Factors in Quality Assurance, John Wiley and Sons, New York, 1969.

60. Kletz, T. A. and Whitaker, G. D., Human Error and Plant Operation, EDN 4099, Safety and Loss Prevention Group, Petrochemicals Division, Imperial Chemical Industries, Ltd., Billingham, England, 1973.

61. McCornack, R. L., Inspector Adequacy: A Study of the Literature, SCTM-53-61(14), Sandia Laboratories, Albuquerque, New Mexico, 1961.

62. Meister, D., Human Factors: Theory and Practice, John Wiley and Sons, New York, 1971.

63. MIL-H-46855A, Military Specification, Human Engineering Requirements for Military Systems, Equipment and Facilities, U.S. Dept. of Defense, Wash., D.C., 2 May 1972.

64. MIL-STD-1472A, Military Standard, Human Engineering Design Criteria for Military Systems, Equipment and Facilities, U.S. Dept. of Defense, Wash., D.C., 15 May 1970.

65. Morgan, C. T., Cook, J. S. III, Chapanis, A. and Lund, M. W. (eds), Human Engineering Guide to Equipment Design, McGraw Hill Book Co., New York, 1963.

66. Rasmussen, J., "Man-Machine Communication in the Light of Accident Records", Proceedings of the International Symposium on Man-Machine Systems, Cambridge, England, 1969.

67. Raudenbush, M. H., "Human Engineering Factors in Control Board Design for Nuclear Power Plants", Nuclear Safety, 1973, 14, 21-26.

68. Ronan, W. W., Training for Emergency Procedures in Multiengine Aircraft, AIR-153-53-FR-44, American Institutes for Research, Pittsburgh, Penna., 1953.

69. Rook, L. W., Reduction of Human Error in Industrial Production, SCTM-93-62(14), Sandia Laboratories, Albuquerque, New Mexico, 1962.

70. Shapero, A., Cooper, J. E., Rappaport, M., Schaeffer, K. H. and Bates, C. J., Human Engineering Testing and Malfunction Data Collection in Weapon System Programs, WADD TR 60-36, Wright-Patterson Air Force Base, Ohio, 1960.

71. Siegel, A. I. and Wolf, J. A., Man-Machine Simulation Models, John Wiley and Sons, New York, 1969.

72. Swain, A.D., A Method for Performing a Human Factors Reliability Analysis, Monograph SCR-685, Sandia Laboratories, Albuquerque, New Mexico, 1963.

73. _____, Some Problems in the Measurement of Human Performance in Man-Machine Systems", Human Factors, 1964, 6, 687-700.

74. _____, "Some Limitations in Using the Simple Multiplicative Model in Behavior Quantification", W. B. Askren (ed.), Symposium on Reliability of Human Performance in Work, AMRL-TR-67-88, Wright-Patterson Air Force Base, Ohio, 1967.

75. Van Cott, H. P. and Kincade, R. G. (eds.), Human Engineering Guide to Equipment Design (Rev. Ed.), U.S. Govt. Printing Office, Wash., D.C., 1972.

76. Williams, H. L., "Reliability Evaluation of the Human Component in Man-Machine Systems", Electrical Manufacturing, 1958, 4, 78-82.

77. Woodson, W. E. and Conover, D. W., Human Engineering Guide for Equipment Designers, Univ. of California Press, Berkeley, Cal., 1964 (2nd ed.).

WASH—1400
(NUREG-75/014)

COMMON MODE FAILURES

Bounding Techniques
and
Special Techniques

APPENDIX IV

to

REACTOR SAFETY STUDY

U.S. NUCLEAR REGULATORY COMMISSION

OCTOBER 1975

Appendix IV
Table of Contents

Section			Page No.
1.	INTRODUCTION AND OVERVIEW		IV-1
2.	COMMON MODES IN EVENT TREES AND FAULT TREES		IV-7
	2.1	Introduction	IV-7
	2.2	Contribution of Event Trees to the Study of Common Mode Failures	IV-7
	2.3	Common Mode Failures	IV-8
REFERENCES			IV-9
3.	BOUNDING AND QUANTIFICATION TECHNIQUES FOR COMMON MODE FAILURES		IV-11
	3.1	Introduction	IV-11
	3.2	Bounding by Smaller Combinations	IV-12
		3.2.1 Basic Considerations	IV-12
		3.2.2 Bounding Combinations of Two Failures	IV-13
		3.2.3 Bounding Combinations of Three or More Failures	IV-16
	3.3	Analyses and Quantifications Applied in the Study	IV-17
	3.4	More Detailed Quantification Approaches	IV-19
4.	FAILURE COUPLING		IV-27
5.	SPECIAL ENGINEERING STUDIES TO IDENTIFY POTENTIAL COMMON MODES IN ACCIDENT SEQUENCES		IV-35
	5.1	Summary of Results	IV-35
		5.1.1 Large LOCA Sequences	IV-35
		5.1.2 Small LOCA Sequences	IV-36
	5.2	Summary of Secondary Failure Methods	IV-37
	5.3	PWR LOCA Sequence Common Mode Failure Evaluations	IV-37
		5.3.1 Sequence CD (Given A or S)	IV-37
		5.3.2 Sequence CDI (Given A or S)	IV-37
		5.3.3 Sequence HF (Given A or S)	IV-38
		5.3.4 Sequence G (Given A or S)	IV-38
		5.3.5 Sequence AD (Given A)	IV-38
		5.3.6 Sequence CF (Given A or S)	IV-39
		5.3.7 Sequence B (Given A or S)	IV-39
		5.3.8 Sequence F (Given A or S)	IV-40
		5.3.9 Sequence HI, FI, or HFI (Given A or S)	IV-40
		5.3.10 Sequence HG (Given S)	IV-40
		5.3.11 Sequence D (Given S)	IV-40
	5.4	Supporting Material	IV-41
		5.4.1 Summary of the Results of Examining Inter-System Interfaces for Sequence Failure Possibilities	IV-41
		5.4.2 Summary of Plant Layout Examination for Sequence Secondary Common Mode Failures	IV-41
		5.4.3 Systems Which Can be Failed by Common Mode Failure of Similar Component	IV-42

Table of Contents (Continued)

Section		Page No.
6.	SPECIAL ENGINEERING STUDIES TO IDENTIFY POTENTIAL COMMON MODES IN ACCIDENT SEQUENCES	IV-45
	6.1 Summary of Results	IV-45
	6.1.1 Large LOCA Sequences	IV-45
	6.1.2 Small (1) and Small (2) LOCA Sequences	IV-45
	6.1.3 Transient Sequences	IV-46
	6.2 Summary of Methods	IV-46
	6.3 Consideration of Common Mode Effects in Particular Sequences	IV-47
	6.3.1 Large LOCA	IV-47
	6.3.1.1 Sequence AE - LLOCA/ECI	IV-47
	6.3.1.2 Sequence AI - LLOCA/LPCRS	IV-47
	6.3.1.3 Sequence AJ - LLOCA/HPSW	IV-47
	6.3.2 Small LOCA's	IV-47
	6.3.3 Transients	IV-47

List of Tables

Table		Page No.
IV 1-1	Common Mode Treatment in the Various Analysis Stages	IV-5/6
IV 3-1	Classes of Potential Common Mode Mechanisms	IV-25/26
IV 3-2	Combination Properties Indicating Potential Common Cause Susceptibility	IV-25/26
IV 4-1	PWR Coupling - BWR Coupling	IV-31/32
IV 5-1	Similar Component Failures and Significant Affected Sequences (Large LOCA)	IV-43/44
IV 5-2	Interface Examination Results	IV-43/44
IV 5-3	Electrical Power Interfaces	IV-43/44
IV 6-1	Sequence AE-LLOCA/ECI, Principal Common Mode Possibilities and Effects	IV-49/50
IV 6-2	Sequence AI-LLOCA/LPCRS, Principal Common Mode Possibilities and Effects	IV-49/50
IV 6-3	Sequence AJ-LLOCA/HPSW, Principal Common Mode Possibilities and Effects	IV-51/52
IV 6-4	Sequence S_1E-Small LOCA (1)/ECI, Principal Common Mode Possibilities and Effects	IV-51/52

List of Figures

Figure		Page No.
IV 4-1	Independent Versus Coupled Failure Rate Distributions [Frequency on Vertical Axis (Ordinate), Failure Rate on Horizontal (Abscissal)].....	IV-33/34
IV 4-2	Increased System Uncertainties Due to Coupling Effects (Vertical Axis - Frequency; Horizontal - System Probability).....	IV-33/34

Section 1

Introduction and Overview

With regard to the analyses performed in this study, potential common mode failures can be defined as multiple failures which are dependent, thereby causing the joint failure probability to increase. The multiple failures are common mode or dependent because they result from a single initiating cause, where "cause" is used in its broadest context.

The single initiating cause can be any one of a number of possibilities: a common property, a common process, a common environment, or a common external event. Multiple failures which are dependent can likewise encompass a spectrum of possibilities such as multiple system failures caused by a common component failure, system failures caused by a common external event, multiple component failures caused by a common defective manufacturing process, a sequence of failures caused by a common human operator, etc.

Because potential common mode failures entail a wide spectrum of possibilities and enter into all areas of modeling and analysis, common mode failures cannot be isolated as one separate analysis, but instead must be considered throughout all the modeling and quantification steps involved in the risk assessments. In the study, common mode considerations were incorporated in every stage of the analyses. Table IV 1-1 gives a general breakdown of common mode treatments that were performed as an integral part in each of the analysis steps.

This appendix will describe in detail only those aspects of the common mode failure methodology which are not discussed in other portions of the report. Bounding and coupling techniques, in particular, will be described (pertaining to Table items III-2, III-3, IV-2, and IV-3 of Table IV 1-1) and special engineering investigations conducted to identify additional potential common mode failures are discussed in section 5-1 of this appendix. Specific examples and applications pertaining to all the above items are also described throughout the fault tree and event tree appendices.

Before discussing the bounding techniques and special investigations, a review of the overall common mode methodology will be given here to place the material of this appendix in better context. A fuller discussion of the overall common mode methodology is found in Appendix XI and the Main Report.

Following the outline of the table, the event tree constructions first treated common mode failures in their detailed modeling of system to system functional interactions. If failure of one system caused other systems to fail or be ineffective, then this was explicitly modeled in the event trees by drawing straight lines through the other system columns.[1] These straight lines had no steps for the affected systems and hence did not require consideration of possible interaction with these eliminated systems.

The systems rendered failed or ineffective by the single system failure were treated in the subsequent analysis as being essentially non-existent, and the analysis then concerned itself only with the critical single system failure. By considering these functional interactions, multiple system possibilities were thus changed to single system failure analyses. From a common mode viewpoint, the affected systems constitute common mode events which are coupled to the single system failure. Incorporation of this coupling in the event trees was most significant since it in essence changed a product of system probabilities into one, single system probability. The impact of the event trees on this type of common mode dependency can be gauged by the numbers given in section 2 of Appendix I which show the reduction in size for the event trees constructed in the study, which incorporated dependencies, as compared to the unconstrained size obtained when dependencies are not considered.

In addition to incorporation of system interdependencies, the event trees also defined the context for which the individual fault trees were to be constructed. Particular system failures, i.e., the top events of the fault trees, were defined within the context of other

---

[1] See Appendix I for event tree descriptions.

particular systems having already failed. The fault trees in an accident sequence were coupled by the system failure definitions and by the common accident conditions (the fault trees were thus conditional fault trees).[1]

The construction of the fault trees included common mode considerations in determining the level to which failures should be analyzed and the failure causes and interfaces which should be modeled. The fault trees were constructed to a level of detail such that all relevant common hardware in the systems would be identified. Because of this depth of analysis, single failures were identified that would cause multiple effects. These included potential single failures that could cause several systems to fail or be degraded and that could cause redundancies to fail or be negated. Had the fault trees stopped at a less detailed level, these single failures would have had to be treated as common mode causes and given special common mode treatments since they would not have been explicitly shown in the fault trees.

The failure causes modeled in the fault trees included not only hardware failure but also failures caused by human intervention, test and maintenance acts, and environmental effects, which enabled potential dependencies to be investigated and incorporated in the quantification. To illustrate the effects of this more complete failure cause identification, in a number of the fault trees constructed, a valve being in a closed position was determined to be a failure. The failure could be caused by the valve itself failing closed, i.e., a hardware failure, and this cause is the cause usually included in the fault tree model. In addition to the valve hardware failure, however, the valve could also be in a closed position due to its being purposely closed for testing or maintenance and it could also be in a closed position due to the operator's forgetting to open it after the previous test or maintenance act. These other causes are often ignored in fault tree modeling; however, they have the same effect on the system as the hardware failure. These other causes were included in the analysis of the fault trees for the study, and in certain cases they had much higher probability contributions to system failure than the hardware causes. In a number of cases these non-hardware contributions gave significantly high system failure probabilities (essentially single failure probabilities) such that all other contributions had minor impact on the system number.

In addition to their individual impacts, the non-hardware contributions were examined in the quantification stage for possible interdependencies. Multiple failures caused by human errors were dependent if the same operator could perform all the acts. Testing or maintenance caused failures to be dependent if several components could simultaneously be brought down for testing or maintenance. Accident environments caused multiple failures to be dependent if the failures could be due to the same environment. Identification of non-hardware causes laid the basis for individual and dependent event calculations which were performed in the quantification stage, and the resulting significance can be seen by the large contributions predicted for non-hardware causes.

The fault tree quantification stage, also tended to implicitly cover dependency and common mode considerations within the basic calculations. The component data which were input to the calculations were total failure data and had error spreads (probable ranges) to account for uncertainties and variations. The failure rate for a particular component included not only contributions from hardware failure (sometimes called the random failure rate), but also contributions due to testing or maintenance, human causes, environment causes, etc. The error spreads aided in covering uncertainties not only from statistical estimation but also from possible defects in the component, possible failure mechanisms not included in the data sources, and from other physical causes of possible variations. This realistic treatment of data gave higher system failure probabilities, which often proved to be insensitive to common mode effects when sensitivity studies were performed.

The quantification formulas treated both hardware and non-hardware contributions with their relevant dependencies. The human errors and test and maintenance downtime contributions identified in the fault trees were quantified to obtain

---

[1] The definition and probability quantification of the containment failure modes, incorporating accident dependency considerations, are given in Appendices V and VIII.

their probability contribution. Error spreads were used for human probabilities to account for individual variations and possible inefficiencies (tiredness, possible confusion, etc.). A log-normal distribution was used to obtain test and maintenance downtimes, where the distribution is positively skewed (having a tail for longer downtimes) to account for test and maintenance problems, possible laxities, and other test and maintenance associated deviations. When human or test and maintenance contributions had additional interdependencies, coupling formulas using the log-normal median approach were employed. Accident environment effects on both components and human responses were treated by using higher failure rates when appropriate and coupling individual failures when the same environment affected the failures.[1]

In the fault tree quantification stage, error spreads were propagated through the calculations to determine the resulting error spreads on the computed system probabilities. The system error spreads thus included the possible deviations in test and maintenance, human errors, and failure rates which thereby caused other potential common mode effects not explicitly included to have less impact since they now needed to lie outside the error spreads. Bounding and coupling calculations were also performed throughout the quantification to determine maximum possible impacts from common mode failures which might exist and were not previously included. The bounding and coupling studies served as an additional check on the calculations and identified areas that needed further investigation because of their larger possible impact. Failure rates were also coupled to determine the potential effects of several components all having a high failure rate due to a bad manufacturing batch, quality control error, etc. Since the bounding and coupling techniques were not described in detail in the modeling and analyses appendices (Appendices I, II, III, and V), they are treated in this appendix.

After the fault trees were quantified, the event tree quantification stage combined the individual fault tree probabilities to obtain sequence probabilities. To obtain the sequence probabilities, Boolean techniques were used on the fault trees to extract any components which were common to several systems in the sequence. Single failures that could fail multiple systems were thus identified and quantified, and as a result independent system failures became dependent failures.

Since an accident sequence in the event trees can be viewed in terms of fault tree logic, the same quantification techniques were used on the individual fault trees. (In terms of fault tree representation, the individual systems in a sequence are viewed as being inputs to an AND gate to form the accident sequence.) Human errors, test and maintenance, and accident environment were evaluated for their contributions to the sequence, and the contributions were coupled when they were dependent. Since multiple systems were analyzed, the couplings now included dependencies across systems.

For the consequence calculations, the accident sequences were partitioned into release categories.[1] The probabilities for sequences assigned to the same category were then summed to obtain the total release category probability which was used as the input for the final consequence calculations. The grouping tended to cover effects of dependencies and common modes since single system failures often existed in each release category. Multiple failure accident sequences thus became negligible, even with possible common modes, when they were added to the single failure accident sequences to obtain the total release category probability. Bounding and error propagation techniques were used on the multiple failure accident sequences to investigate maximum common mode effects. The bounding techniques encompassed those used for the fault trees, which are described in this appendix.

As a final check on possible dependencies and common mode effects, special engineering investigations were performed to complement the modeling and mathematical techniques which had been used throughout the study. The event tree accident sequences which were judged to be possible susceptible to common mode impacts which had not been identified were reexamined for any extraneous dependencies which may have been previously overlooked. These sequences were also examined to determine

---

[1] See Appendix II for detailed applications and discussions.

[1] Appendix V.

potentials for interdependencies between initiating events and system failures. As part of the common mode investigations, a design adequacy task investigated the effects of earthquakes and external events. The fault tree and event tree models were also reviewed, and checks were made comparing model predictions versus available past history experiences. The comparisons with past history are contained in the data and fault tree appendices. As stated, since they are not contained in the other appendices, the accident sequence special investigations are described in this appendix.

With regard to the impact of common mode failures on the spectrum of individual results computed in the study, in many areas common mode contributions had significant effects and in some areas they did not. This conclusion may not seem simple, however, many different detailed results were computed in the study to arrive at the final risk assessments.[1]

In the accident sequence definitions and in the containment failure mode analyses, common mode considerations had a significant impact. Common mode considerations of functional interdependencies significantly modified the event tree sequences and hence the resulting probabilities. Consideration of containment failure mode dependencies gave significantly modified probability values to be used for the accident sequences.

In the fault tree and event tree quantifications, common mode failures in many cases did not have as significant an effect. Single system failure probabilities dominated the accident sequences which determined the release category probabilities, and single component failures, in turn, dominated the single system failure probability. Common mode failures between components thus had little impact since at most they could change multiple component failures into single component failures and these already existed for the system.

Human errors, because of their larger basic probabilities as compared to component failure rate data, in a number of cases dominated the system again causing common modes between components to have a small effect.

In certain systems, however, common mode contributions did significantly enter, for example, in cases when several failures were coupled to a common human cause. There were other cases in which common modes did impact, either through the fault tree development and fault definition or through the quantification. These specific cases, along with the specific event tree findings, are discussed in their appropriate sections (Appendices I, II, and V).

The outcomes of the varying significance of common mode failure which were found in the study further reinforce the requirement that common modes and general dependency considerations should not be isolated and treated separately, but should be incorporated throughout all stages of the analysis. However, this along with all the other modeling considerations, is what should be automatically done in any thorough and complete analysis.

---

[1] If one looks specifically at the final risk assessment numbers then common modes in general had a very significant effect as discussed in Appendix XI and the main report. (In large part, this was due to the event tree effects.)

TABLE IV 1-1 COMMON MODE TREATMENT IN THE VARIOUS ANALYSIS STAGES

I. EVENT TREE CONSTRUCTION

1. Incorporation of functional dependencies between systems in the sequence constructions.
2. Establishment of accident sequences including containment failure mode definitions which incorporate system and accident interdependencies.

II. FAULT TREE CONSTRUCTION

1. Resolution of failures to a level such that common system hardware will be identified.
2. Fault tree construction which identify human interfaces, test and maintenance interfaces, and other interfaces of potential dependency.

III. FAULT TREE QUANTIFICATION

1. Practical data utilization, which incorporates uncertainties and variations.
2. Quantification formulas which incorporate dependencies and contributions due to human error, test and maintenance, and accident related environments.
3. Mathematical techniques involving bounding calculations and error propagation calculations, which serve to determine the significance of possible dependencies and serve to incorporate resulting uncertainties.

IV. EVENT TREE QUANTIFICATION

1. System fault trees combined and analyzed by Boolean techniques to extract common components between systems.
2. Quantification formulas which incorporate couplings and dependencies across systems due to human error, test and maintenance, and accident environments.
3. Grouping of accident sequences of similar outcome and identification of the dominant accident sequences using discrimination and bounding techniques.

V. SPECIAL ENGINEERING INVESTIGATIONS

1. Investigation of special, susceptible accident sequences to determine any remaining possible common modes including those due to external events and common component sensitivities.
2. A special design adequacy task to investigate common mode failures resulting from earthquakes, other external forces, and post accident environments.
3. Final checks on the fault tree and event tree models for model accuracy and consistency.

Section 2

Common Modes in Event Trees and Fault Trees

2.1 INTRODUCTION

For the convenience of the reader, excerpts of the common mode discussions in Appendices I and II are reproduced here. (The bounding techniques and special engineering investigations are given in the following sections.) For further specific details, the fault tree and event tree quantification sections include discussions and considerations applicable to common mode failures when they were significant contributors.

2.2 CONTRIBUTION OF EVENT TREES TO THE STUDY OF COMMON MODE FAILURES

The potential effects of common mode failures (CMFs) on the safety of nuclear power plants have been increasingly discussed in recent years. Current design requirements related to safety address this matter in certain areas, principally with regard to possible external forces due to natural phenomena and airplane crashes. This is because a large external force such as an earthquake might not only initiate an accident but also result in failures of engineered safety features provided to mitigate the accident. Therefore, all the systems that contribute to assuring the safety of the plant (e.g, the reactor coolant system and all the ESFs) are designed to withstand substantial earthquakes without failure (Ref. 1). In addition to the above, LOCAs can impose large reaction forces and cause missiles which have the potential to damage components whose failure can interfere with the performance of ECCs and other ESFs. This has led to the use of pipe restraints, missile shields and other such design requirements to prevent damage by the LOCA. Beyond this, limited analysis has been done to quantify the effects of potential common mode failures on reactor accidents.

An important objective of this study has been to develop methodologies suitable for quantifying the contribution of common mode failures to reactor accident risks. Event trees play a role in CMF studies because they eliminate illogical and meaningless accident sequences. Evaluation of potential CMF contributions requires examination of the potential CMF interrelationships of the various events in each accident sequence; any sequences that can be eliminated need not be examined. The disciplined examination of the function-to-function, function-to-system, and system-to-system interrelationships in the specific context defined by the accident sequences has made a key contribution in limiting the magnitude of the CMF effort needed in this study.

A measure of this contribution is comparison of the number of interactions possible with the number actually involved. This can be done, for instance, by examining the large LOCA and containment event trees described above for the PWR and BWR. The PWR trees have 8 and 5 headings, respectively; the BWR, 9 and 7. Use of 2^{n-1} tree with all possible permutations and combinations of choices included would give roughly 4000 accident sequences for the PWR and 32,000 for the BWR. Since each sequence would have 12 and 15 elements, respectively, the number of potential CMF interactions to be investigated would be about 48,000 for the PWR and about 480,000 for the BWR. However, the PWR and BWR large LOCA and containment event trees involve only about 150 sequences each, with an average of about 10 potential interactions per sequence. Thus the total number of potential interactions for the PWR and BWR would be about 1500 each, or a reduction from the 2^{n-1} approach of about a factor of 32 for the PWR and 320 for the BWR.

Thus, for the large LOCA, the use of event trees has eliminated illogical and meaningless combinations of events and thus reduced the areas requiring examination for CMFs by about three orders of magnitude. This approach contributes enormously to making the analysis of potential CMFs tractable.

In considering the total number of event trees involved in the overall study (see sections 4 and 5 of this Appendix), it can be seen that many thousands of potential accident sequences involving hundreds of thousands of potential interactions were screened in this study to arrive at a relatively small number of potential CMF interactions. As will be shown in later Appendices (IV and V), further screening involving the identification of those particular sequences which were the dominant

contributors to risk reduced the number of potential interactions of interest by additional very large factors.

In addition to the above, it should be noted that the containment trees discussed in Appendix II represent an extensive common mode failure investigation of the relationship between core melting and containment integrity. While it has long been known that a molten core would almost surely result in loss of containment integrity, this study has shown that there are widely different consequences having widely different probabilities for the various modes of containment failures.[1]

2.3 COMMON MODE FAILURES

Hardware failures, human errors, and test or maintenance outage all have a direct effect on the probability of system failure (i.e. the unavailability or unreliability). System failure probabilities can also be affected by more subtle factors such as common environment, common design, common manufacturing processes, or common human intervention with the system (including operation, maintenance, and their associated test procedures). All of these common links represent potential dependencies which can compromise any assumptions of independence of failures. Events related to common hardware and other single events having direct input to a system are identifiable in the process of constructing the fault tree as described in Appendix II. The component failure event RWST 1CS-TK-1 "Rupture" (common hardware) and fault event "RWST Vent Plugged" (direct input event) as shown in the Containment Spray Injection System (CSIS) example (See Appendix II section 5.4) are events that lead to multiple system and subsystem failure. The PWR refueling water storage tank (RWST) is common to both CSIS subsystems and also to the emergency core cooling injection systems. Rupture of the RWST or plugging of the RWST vent would fail the two CSIS subsystems and the low pressure injection system (LPIS) of the emergency core cooling systems.

Other types of events identified on the detailed fault trees may have common mode failure implications but require further investigation to determine if they are probable. For example, the third level event on the CSIS detailed tree "Containment Pressure Sufficiently High to Reduce Spray Effectiveness" is a common mode suspect since the event appears as an input to both redundant subtree branches. If upon further investigation (relating CSIS design output pressure with the maximum pressure which might be attained in the containment) the event is determined to be probable, then the event is a common mode contributor since it is a single event that can fail both spray subsystems. Further investigation of this event, however, indicated that it would be unlikely to occur; that is, the containment pressure will not reach a level sufficiently high to reduce CSIS effectiveness. The event was, therefore, not shown on the reduced tree which was quantified.

Some human interactions with a system, whether for operation, test, maintenance, or calibration are potentially important common mode events. In constructing the detailed fault trees operational errors which can cause components not to be in their proper operational state when required are shown as individual events on the tree (e.g., "Operational Error - Switch S8 Not Closed," "Operational Error - Valve 506 Closed," etc.).

In the process of evaluating the fault trees, functionally related human error events were examined to determine their potential for common mode failure. For example, four human error events, each related to failure to start one of four redundant BWR high pressure service water pumps, were examined to determine whether those errors were likely to be committed independently or as a single act. The major contributor to BWR high pressure service water system failure as determined in the analysis was failure of the operator to turn on one or more of the four redundant pumps when the system is needed. If the operator does not start one pump, there is a high probability that he will not start the other pumps as well.

Human errors related to the testing and maintenance of components can also be important common mode contributors. For example, instruments can be "valved-out" for calibration purposes and not restored to their operational state when the calibrations are complete, valves can be aligned to divert pump flow during a test and not realigned following the test, reset switches may not be depressed following logic test, etc.

All components in a system can be potentially coupled to common environmental

[1] See Appendices V, VI, VII, and VIII.

causes for failure by expanding the fault tree analysis into secondary causes, i.e., by postulating possible causes for component failures which exceed the design ratings of the components and then developing the fault tree to identify possible causes for those secondary events occurring. For example, the analyst, knowing that a relay is rated for 180°F, would show an event on the fault tree which states, in essence, that "relay fails due to temperature >180°F. The fault tree would be developed, then, to identify possible causes for the temperature exceeding 180°F. The fault tree would be similarly developed about other environmental conditions which would cause the relay to fail. Some of the events could be common to other component failures and, therefore, would be common mode events.

To develop a fault tree indiscriminately into common mode or secondary causes without regard to the likelihood of occurrence results in a large number of events that must be subsequently discarded because of their insignificance, thus causing a considerable waste of time and effort. In order to assure that adequate consideration was given to common mode causes of system or subsystem failure an initial screening of component failure events was made, and those events which have potential for contributing significantly to common mode system failure were examined and analyzed further. The approach used for this initial screening of events in search of common mode contributors is as follows:

> System fault trees and drawings were reviewed to identify multiple components and their respective failure modes that would be most likely to contribute to system and multiple system failures. In general those components selected for further consideration were redundant operating partners (components of the same type operating in parallel whose failure could fail the system). Components of the same type and manufacture were retained for further consideration on the basis that those components could potentially be more likely to have common latent defects. Also, like components would more likely be subjected to common operational, maintenance, and testing procedures, etc., that could contribute to common mode failures.
>
> Components that could potentially be affected by a common operating environment were examined relative to their proximity to one another and to energy releasing sources (rotating machinery, flammable fluids, steam lines, etc.) within the plant. A determination was made as to whether energy was likely to become released or not and, if released, whether or not multiple components would likely be affected. Among the items considered were the amount of energy which could be released, physical barriers between components and the energy sources, the vulnerability of components to the forms of energy that could be released, the modes in which the components would need to fail in order to fail systems, and the manner and time in which corrective action would or could be taken.

The event coding scheme described in Appendix II facilitates the sorting of events having a common property. For example, human error events related to manual valves in a system can be retrieved by sorting for valve type MX and fault mode designator X. In some cases the fault tree analyst may decide that two or more components may be subject to common events due to their proximity to an energy source, or their being subjected to the same maintenance procedure, etc. Because of location in a large fault tree, it is not immediately clear whether the potential dependency is important or not. In the process of analysis the analyst will give the components the same name. Later, when the fault tree is processed for evaluation, it can then be determined whether the common mode is potentially significant.

In addition to the fault trees themselves, common mode failures within a system are accounted for in the methods of quantification used for the tree; common failures which affect multiple systems are accounted for in the event tree quantifications. These quantifications are discussed in Appendix IV and in the individual fault tree quantifications.

References

1. AEC General Design Criteria, Appendix A, Title 10, Code of Federal Regulations, Part 50, Criterion No. 2.

Section 3

Bounding and Quantification Techniques for Common Mode Failures

3.1 INTRODUCTION

As stated previously, common mode failures can be defined to be multiple failures which occur because of a single initiating or influencing cause. The single cause or mechanism serves as a common input to the failures affected. If this mechanism or cause occurs, all the failures are triggered and a common mode failure occurs. The components affected by the common mechanism or cause may constitute hardware, systems, subsystems, or particular events.[1]

Examples of common mode failures are numerous. Two spring loaded relays in parallel fail because of a common design defect. The defect causes both relays to simultaneously fail and is the common cause. Because of an error of incorrectly disengaging the clutches, three motor valves are placed in a failed state after maintenance. The common cause for the valve failures is the common maintenance error. A steam line ruptures causing multiple circuit board failures. The common mode failures are the circuit board failures and the common cause is the steam line rupture.

Instead of triggering simultaneous failures, which is the extreme case, the common cause may produce a less severe, but common, degradation of the components. The components do not simultaneously fail together; however, their joint probability of failure can be greatly increased. In this degradation situation, the second component, for example, may fail at a time later than the first component failure. Because of the common impressed cause, however, the second component failure is dependent and coupled to the first failure. The joint probability of failure of the two components can consequently be much higher than the product of the individual component probabilities (the independent failure situation).

Numerous examples can again be given for occurrences of degradation common mode failures. Because of harsh accident environment, two pumps become degraded in performance. Given one pump has failed due to this environment, there is a high probability that the second pump will also fail. The second pump may not fail immediately when the first pump fails. However, the probability for the second pump's failing is now higher than its unconditional failure probability. The second pump, for example, may not fail at the same time, but there may be a high probability it will fail near the first pump's failure time.

In the above example, the common mode or dependent failure is the failure of the two pumps and the common cause is the harsh environment. Another example in the same general category is a failure induced by a test or maintenance error. Because of improper maintenance and calibration, three motor valves become degraded in performance.

Depending upon the extent of the test or maintenance error, the valves may suffer minor degradation to complete inoperability. Even if the degradation is not severe, their joint failure probability will increase. In conjunction with this increase in probability, the failure dependence of the valves will be increased due to the common test or maintenance.

Another example of common mode failures of the degradation type is the loading or dragging effect caused by another failure. Three pumps are operating and one fails. Because of this failure, the other two pumps suffer a degradation due to the extra load placed upon them. Their failure probability will then be higher than their joint unconditional probability of failing.

For this pump loading example, the common mode failures are the failures of the second and third pumps. The common cause is the failure of the first pump. The common causes may be compounded, for example, if, in addition, the three pumps are located in a harsh accident environment. An additional common cause is then the environment imposing its own degradation.

---

[1] The term "component" may therefore, be interpreted in the general sense, referring to any basic failure being considered.

If a common cause occurs, the failures of the affected components must be treated as dependent events and not as independent events. In conjunction with the dependency of the events, the times of failure of the affected components are also coupled to one another. To quantify common mode failures, statistical and reliability methods must therefore be employed which treat dependencies in failure occurrences. In particular, conditional probabilities and conditional failure distributions must be analyzed and be combined. A number of techniques can be used, certain of these which are considered to be the most straightforward and which were applied in the study.

It should be noted that common mode failures do not encompass all the degradation phenomena or all the dependency phenomena which exist in any real life situation. For those types of degradation and dependency which are not modeled explicitly as common modes, the techniques to be described may not be applicable. Even for common mode type failures, other techniques may be used which better model a particular phenomenon.

A technique, for example, is described in a later section where a particular type of degradation is modeled by simultaneously increasing all affected component failure rates. The components now all fail with a greater failure rate. The effect of this degradation is incorporated in the error bounds of the system failure probability. That model is useful for incorporating and investigating manufacturing defects, certain maintenance errors, and certain environmental effects.

Other types of degradations, which may not be common mode associated, include certain types of wear-out phenomena and drifting phenomena. If these phenomena are judged pertinent to the problem, then other approaches may need to be used.

The techniques in the next sections describe methods by which a maximum bound can be placed on the contribution from common mode failures. These bounds have importance, for example, in determining the adequacy and believability of other contributions which have been computed in a quantification analysis (such as the independent failure contributions). If data are available, more exact calculations of common mode contributions can be performed. These calculations are also discussed.

3.2 BOUNDING BY SMALLER COMBINATIONS

3.2.1 BASIC CONSIDERATIONS

One of the first questions to be asked is whether common mode failures can have an impact on a particular quantitative evaluation. A general technique is first described by which an upper bound, or maximum value, can be obtained for the common mode failure contribution. The upper bound technique, which will be called "combination bounding", has the advantage of being relatively simple to apply. It can therefore be used as a preliminary check to determine possible impacts. If the upper bound, which represents a maximum possible effect, does not significantly change a predicted system failure probability, then the number is insensitive to common mode contributions. If the upper bound does change and increase the result, then more detailed analyses need to be performed to determine the actual effect of common mode failures.

As is true in any bounding approach, instead of serving as a check, the upper bound itself can be used as a result. For example, if the upper bound satisfies specification requirements, then no further analysis need perhaps be performed. Alternatively, if error bars or uncertainties are given for a system result, these error bars can be increased to account for a maximum possible common mode effect.[1] If the increased uncertainties still satisfy accuracy requirements, then further analysis may not be needed.

The upper bounds can finally be used to help direct and scope general common mode failure investigations. The upper bounds represent a maximum effect and hence a list of candidate common mode failures can be ordered with regard to their respective upper bounds. The common mode failures having the largest upper bounds can have the maximum effect and hence these are analyzed and investigated first.

Although the combination bounding technique is simple in principle, it does have the disadvantage in a number of situations of giving too conservative a result (i.e., too large of an upper

---

[1] In a statistical sense, the error bars and uncertainties would thus account for systematic-type errors as well as random-type errors.

bound). Other sections will discuss techniques by which better and hence tighter bounds are obtainable for common mode failure contributions. If the data are available, techniques are also discussed for computing exact common mode contribution.

3.2.2 BOUNDING COMBINATIONS OF TWO FAILURES

Since common mode approaches are not normally found in the literature, this discussion will be somewhat basic. The reader with a background in probability can skim over this section, referring principally to the result obtained [Equations (IV 3-6) and (IV 3-20) through (IV 3-22)]. Section 3.3 treats applications in the study and section 3.4 deals with more involved modeling.

The bounding technique is given the name combination bounding because smaller valued combinations or redundancies are used for establishing the bounds. Consider the event of both A and B failing and denote this joint failure occurrence by AB. The expression AB thus represents the combination of A and B both failing. The symbol A and the symbol B may for example represent failures of particular components and the expression AB then represents both of these components failing.

Let the probability of A failing be denoted by P(A) and the probability of B failing be denoted by P(B). For the combination AB, denote its probability by P(AB);

P(AB) = the probability of both A and B failing.

(IV 3-1)

The probability expression P(AB), which will be called the combination probability, is completely general and as such implies nothing about the independence or dependence of A and B.

If A and B are independent, the combination probability, P(AB), can be expressed as the product of the individual probabilities P(A) and P(B);

$$P(AB) = P(A)P(B), \text{ A and B independent} \qquad \text{(IV 3-2)}$$

If the events are not independent and can be due to a common cause, then in general the above equation is not true and the combination probability is not the product of the individual probabilities.

$$P(AB) \neq P(A)P(B), \text{ A and B dependent} \qquad \text{(IV 3-3)}$$

However, even in the dependent case, in order for AB to fail, A must individually fail and B must individually fail. Therefore, in all cases, both independent and dependent;

$$P(AB) \leq P(A) \qquad \text{(IV 3-4)}$$

and

$$P(AB) \leq P(B) \qquad \text{(IV 3-5)}$$

Since both inequalities are true, the minimum of either P(A) or P(B) may be taken as the best upper bound;[1]

$$P(AB) \leq \text{MIN}[P(A), P(B)] \qquad \text{(IV 3-6)}$$

Therefore, MIN[P(A), P(B)] denotes the minimum, or smallest value, of P(A) or P(B). Equation (IV 3-6) thus gives the upper bound obtained by the combination bounding technique. This equation is applicable to the spectrum of common mode failures, from simultaneous triggerings to minor degradations.

In Equation (IV 3-6), P(AB) can represent the total probability of A and B failing from all mechanisms, both random and common mode. The equation therefore gives an upper bound and conservative estimate on the total, true probability of the combination failing. Since Equation (IV 3-6) applies when P(AB) represents the total probability for AB, it therefore also applies when P(AB) represents the probability of a particular common mode failure of AB.

The probabilities and failure events are general representations and can be particularly interpreted and applied to any specific calculation. If A and B are unavailability related failures then P(A), P(B), and P(AB) are availabilities

---

[1] In terms of Boolean theory, AB is a subset of A and is also a subset of B. Therefore, Equations (IV 3-4) and (IV 3-5) follow. The results can also be obtained using conditional probabilities, e.g., for Equation (IV 3-4), $P(AB) = P(A)P(B/A)$ and since $P(B/A) \leq 1$, therefore $P(AB) \leq P(A)$. The quantity P(B/A) is the probability of B, given A has occurred.

(denoted by Q's in the earlier appendices). If A and B are operationally related failures then the probabilities can be interpreted as being failure probabilities or cumulative probabilities, which may be time dependent.

As an example of the use of Equation (IV 3-6), assume a system has been analyzed and evaluated to obtain a system probability number. Among the contributions that cause system failure is the failure of two pumps to start when demanded. There is concern because the investigation has shown that the two pumps may be susceptible to common mode failure. (Possibilities of common causes include, for example, design defects and environmental degradation). For this problem, the possible impact of the common mode contribution is desired in order to compare with the system number which has been obtained.

With regard to the two pumps let A now be the failure of one pump and B be the failure of another pump. From the data base (Appendix III), the probability of one pump failing to start when demanded is 10^{-3}.

Thus,

$$P(A) = 10^{-3} \qquad \text{(IV 3-7)}$$

and

$$P(B) = 10^{-3} \qquad \text{(IV 3-8)}$$

If the pump failures are independent, the probability of both failing to start, P(AB), is simply the product of the individual pump probabilities; i.e., $P(AB) = 10^{-3} \times 10^{-3} = 10^{-6}$. However, if the pump failures are due to common causes, Equation (IV 3-6) can be applied and hence,

$$P(AB) \leq \text{MIN}[10^{-3}, 10^{-3}] \qquad \text{(IV 3-9)}$$

or

$$P(AB) \leq 10^{-3} \qquad \text{(IV 3-10)}$$

since 10^{-3} is the minimum individual pump probability (both individual pump probabilities being equal). Therefore, using combination bounding, an upper bound of 10^{-3} is obtained for the combination probability P(AB).

Having obtained an upper bound of 10^{-3}, this number can then be compared to the total system failure probability. If the system probability is of the order of 10^{-3} or larger, then the system is insensitive to this common mode contribution, even at its maximum value. If the system probability is significantly smaller than 10^{-3}, additional analyses would need to be performed to verify independence or to better define the degree of possible common cause dependency.

Instead of serving as a check, the upper bound of 10^{-3} may itself be used in the evaluations. This bound, for example, can be used in the system quantification to determine whether the system failure probability will contribute to the overall risk, even with this maximum common cause contribution. Alternatively, if extreme accuracy is not required and error bars or probability ranges, are associated with the system result, they can be increased to account for the possible maximum 10^{-3} contribution.

As a further example of this bounding technique consider two failures A and B, where now $P(A) = 10^{-5}$ and $P(B) = 10^{-2}$. In the independent case

$$P(AB) = 10^{-5} \times 10^{-2} = 10^{-7}; \quad \text{independent}$$

(IV 3-11)

If common causes are determined to be a possible significant failure mechanism, then Equation (IV 3-6) can be used to give,

$$P(AB) < \text{MIN}(10^{-5}, 10^{-2}) \qquad \text{(IV 3-12)}$$

or

$$(P(AB) < 10^{-5}; \text{ dependent} \qquad \text{(IV 3-13)}$$

since 10^{-5} is the minimum individual probability. Whereas assuming independence, the probability of A and B failing is 10^{-7}; even if common causes are significant, the probability is still less than or equal to 10^{-5}.

In Equation (IV 3-6) and the aforementioned examples, point values are used for the probabilities and the upper bound obtained is a point value upper bound. If error spreads or probability ranges are used in the calculations, then these can be incorporated in the upper bound by using the error spreads or probability ranges in Equation (IV 3-6). If, for example, the upper values of the error spreads are used for the individual probabilities in Equation (IV 3-6), then an upper bound on the combination probability will be obtained which now incorporates the uncertainties in the individual probabilities.

In the preceding example, if factors of 10 error spread are associated with P(A) and P(B), an upper bound on P(AB) can be obtained which now incorporates the uncertainties on P(A) and P(B) if conservative values (upper error spread values) are used in Equation (IV 3-6). For $P(A) = 10^{-5}$ and $P(B) = 10^{-2}$ with factors of 10 error, the conservative values for P(A) and P(B) are $10^{-5} \times 10 = 10^{-4}$ and $10^{-2} \times 10 = 10^{-1}$, respectively. Therefore $P(AB) \leq MIN[10^{-4}, 10^{-1}] = 10^{-4}$ which now incorporates the uncertainties and variabilities on P(A) and P(B). This use of error spreads and conservative values accounts for the possible omission of specifically defined failure mechanisms in individual estimated probabilities as well as uncertainties due to statistical estimation.

In the following discussions, point value calculations will be described. It will be understood, however, that error spreads or probability ranges can be incorporated by using them in place of the point values. In particular, combination upper bounds which incorporate uncertainties can be obtained by using conservative values for the individual probabilities in all the formulas.

For the upper bound in Equation (IV 3-6) the minimum individual component probability is used, and not the maximum, since the combination probability is less than all of the individual component probabilities. Since the combination probability is less than every one of the component probabilities, it is therefore less than the minimum of these probabilities.

The mathematics used in obtaining the upper bound is quite general and depends only upon basic Boolean and set operation properties. Since the same event space is tacitly assumed in these mathematical operations, one must only take care that the individual component probability is applicable with regard to the combination probability. This applicability property is important and needs some elaboration.

The individual component probability, e.g., [P(A)], gives the probability of the component failing by various mechanisms. Likewise the combination probability [P(AB)] gives the probability of the combination failing by its various mechanisms. The dominant component failure mechanisms need not necessarily coincide with the dominant combination failure mechanisms ("dominant" meaning here those that contribute most to the probability). For example, random failures may dominate and contribute most to the individual component probability, while common mode failures may dominate and contribute most to the combination probability.

For the individual component probability to be applicable, i.e., to be able to be used as in Equation (IV 3-6), either of two conditions must be satisfied:

a. The dominant combination mechanisms should be contained in the individual component failure mechanisms which are thereby included in the individual component probability, or

b. The dominant combination mechanisms should cause an insignificant change in the individual component probability if they were included as part of the individual component failure mechanisms.

In the first of the above conditions the combination mechanisms are included among the individual component failure mechanisms. The combination mechanisms may or may not be dominant with regard to the component failures. In the second of the alternative conditions, the combination mechanisms are not included among the individual failure mechanisms; however, if they were, they would cause negligible effect on the overall component probability.

The above two conditions are obtained from standard reliability considerations and can also easily be derived mathematically by decomposing the probability into constituent mechanisms contributions. In practice, the conditions can be checked before the upper bounds are computed. For example, if common mode failures due to design defects are being investigated, then the component failure probability should contain design defects in its contributions. If the component probability does not cover failures from design defects, then, alternatively, design defect failures should be insignificant with regard to other types of failures affecting the individual component which are covered by the component probability.

As another example, if common mode failures due to environmental degradation are being analyzed and bounded, then the individual component probability should apply to this environment or should be negligibly affected by it. In this example and the previous one, only one mechanism is of interest. The same applicability checks are used when a

series of mechanisms can enter into a number of possible common mode failures.

To bound a number of common mode failure contributions due to a possible group of mechanisms, the component probability should contain and cover this group of mechanisms as they affect the individual component. Alternatively, with regard to the individual component, these mechanisms should have negligible effect as compared to other types of failures the individual component may suffer. For this alternative condition, it is again important to note that the mechanisms are assessed with regard to their affect, not on the combination, but on the individual component.

The above applicability conditions can be rephrased with regard to Equation (IV 3-6) giving the upper bound on P(AB). If P(AB) represents a particular common mode probability, then the individual probabilities P(A) and P(B) should therefore contain or be negligibly affected by the particular common mode mechanism. If P(AB) represents the total combination probability, including various common mode mechanisms, then the individual probabilities should contain or be negligibly affected by these mechanisms.

If error spreads or probability ranges are incorporated in the calculations, then the above applicability conditions and discussions apply to the error spreads or ranges. The individual error spreads or ranges should incorporate the uncertainties and variabilities from the mechanisms which affect the combination or should be negligibly affected by these uncertainties and variabilities.

3.2.3 BOUNDING COMBINATIONS OF THREE OR MORE FAILURES

The combination bounding technique has been applied in the previous discussions to combinations consisting of two failures. The technique can be simply extended to combinations consisting of any number of failures. Consider first a combination of three components failing and let this combination failure be represented by the expression ABC. The expression ABC thus represents the failure of A and the failure of B and the failure of C. Let the probability of this combination failure be denoted by P(ABC);

P(ABC) = the probability of A, B, and C failing.

(VI 3-14)

Since the combination consists now of three failures, an upper bound can be obtained by considering either single failure or two failure combinations. Using the same Boolean and conditional probability methods as in the previous section, one obtains for the single failure bound.

Single Failure Bound:

$$P(ABC) \leq \text{MIN } [P(A), P(B), P(C)]$$

(IV 3-15)

In the above equation, the symbol MIN again denotes that the minimum, or smallest value, of either P(A) or P(B) or P(C) is used as the upper bound. To obtain an upper bound for a triple combination probability, one therefore simply uses the smallest individual component probability.

Equation (IV 3-15) is the result yielded by the combination bounding technique, which is mathematically simple. To be able to use this result, the same applicability conditions must be satisifed as for the two combination case; i.e., the combination mechanisms should be contained in the component probability used as the upper bound or should have negligible effect with regard to its other contributions.

In addition to the single bound, P(ABC) can also be bounded by considering combinations of two failures. Treating a particular double combination as an individual failure event, one obtains, using the same appraoches as before,

$$P(ABC) \leq P(AB) \quad \text{(IV 3-16)}$$
$$P(ABC) \leq P(BC) \quad \text{(IV 3-17)}$$
$$P(ABC) \leq P(AC) \quad \text{(IV 3-18)}$$

or

Double Failure Bound:

$$P(ABC) \leq \text{MIN } [P(AB), P(BC), P(AC)]$$

(IV 3-19)

By combination bounding therefore, another upper bound for a triple combination is obtained by taking the minimum of all possible double combination probabilities. This compares with the previous, alternative upper bound which is obtained by taking the minimum of the individual component probabilities. For the double bound, i.e., Equation (IV 3-19), the same applicability conditions hold, where the double combinations are now the individual failure events

("double combination" is substituted for "component" in the applicability conditions).

Either the single failure bound or the double failure bound can be used for the triple combination. The double failure bound will in general give a smaller and hence better value. However, combination probabilities must be computed for this bound, i.e., P(AB), P(BC), or P(AC); and, if common modes dominate these doubles, then the computation may be infeasible.

The minimum probability does not need to be used, since by Equations (IV 3-16) through (IV 3-18), the triple combination is bounded by any double combination probability. The double bound is therefore useful when two of the components are determined to be reasonably independent. For example, if A and B are independent and the common modes involve only C, then Equation (IV 3-16) may be used to obtain

$$P(ABC) < P(AB) = P(A)P(B) \quad \text{(A and B independent)} \qquad \text{(IV 3-20)}$$

In general, for this type of bounding, the upper bound always used is the double combination that can be justified to be reasonably independent.

Using the same approaches as for the double and triple combinations, the combination bounding technique can be applied to a general combination consisting of n failures:

Single Failure Bound

$$P(A_1 A_2 \ldots A_n) < \text{MIN}\,[P(A_1), P(A_2), \ldots P(A_n)]; \qquad \text{(IV 3-21)}$$

Double Failure Bound

$$P(A_1 A_2 \ldots A_n) < \text{MIN}\,[\text{Probabilities of all double combinations}] \qquad \text{(IV 3-22)}$$

Triple Failure Bound

$$P(A_1 A_2 \ldots A_n) < \text{MIN}\,[\text{Probabilities of all triple combinations}] \qquad \text{(IV 3-23)}$$

.
.
.
etc

The various upper bounds are therefore obtained by computing the probabilities of smaller combinations contained in the original, large combination. The upper bounds are obtained, not only for the minimum, but for any smaller combination probability which is computed. For any of these upper bounds, the applicability conditions must again be satisfied by the smaller combination which is used in the equation.

3.3 ANALYSES AND QUANTIFICATIONS APPLIED IN THE STUDY

Because the combination bounding technique is uncomplicated in its mathematics, it can be easily and simply applied. In the Reactor Safety Study, the technique helped to serve as a check and an analysis tool. In its use as a check, upper bounds were computed for combinations of failures where engineering principles and experience suggested that they could be possible common mode failure candidates. These bounds were then compared to the predicted system failure probability to determine its sensitivity to possible common mode contributions. If the bounds had an impact, further investigation was performed and more detailed analyses were undertaken. As will be described, in a number of cases the bounds were also incorporated as part of the uncertainty and variability.

In checking for common mode impacts, one of the first steps was to identify potential common mode mechanisms. These mechanisms can be categorized into various classes, and one such breakdown used in the study is listed on Table IV 3-1.

In the breakdown, on Table IV 3-1, environmental variations include both accident and non-accident environments. Failure or degradation due to an initiating failure includes, for example, an extra load placed on the second pump due to the first failing. It also includes the cases of missile generation and piping ruptures affecting nearby components. Other forces that could potentially cause failure, include such phenomena as fire, floods, tornadoes, etc.

A number of the mechanisms in Table IV 3-1 were also investigated in other aspects of the study. As an example, certain areas relating to design defects (E, G) were analyzed as part of the design adequacy task in Appendix X. Also, functional dependencies were incorporated in the event trees. These other common mode related studies are described in their respective appendices.

For the particular studies undertaken here, in which combination bounding served as one of the tools, the common mode mechanisms in Table IV 3-1 were those not directly covered by the event tree and fault tree efforts. The common

mode mechanisms were analyzed with regard to their effect on the individual system fault trees and their effect on the combined fault trees which the event trees required.

After identification of potential common cause mechanisms, the component combinations were then examined for their susceptibility to these mechanisms. The component combinations which were examined were the critical paths, or minimal cut sets, i.e., those failure combinations that would cause system failure or combined system failures.

A listing of properties indicating potential susceptibility that was used in the examination is given in Table IV 3-2. The letter or letters in parenthesis beside each property refer to the possible common mode mechanisms which can be associated with property (the letters refer to those used in Table IV 3-1).

In examining for susceptibility properties, all components in the combination (i.e., on the critical path) must have been susceptible to the same potential failure mechanism. Conversely, the components having a common potential mechanism must have constituted a failure combination (critical path).

When the susceptible combinations were identified in the examination process, upper bounds were then taken to determine their maximum impact. In the combination bounding process, single failure bounds were principally used. Since the bounding determination was quite simple (using the minimum component probability), the checking was performed in conjuction with the basic analysis and quantification of the fault tree.

In a number of cases, the bounds showed little potential impact, either individually or collectively, on the predicted system failure probability and its associated error bars that had already been obtained. This was attributed to two principal factors: one, the larger magnitude which had already been obtained for the system probabilities, and two, the lesser precision required for the overall risk analysis along with the relatively large widths of the system error spreads.

The magnitude factor can be seen heuristically. For the system and combined fault trees, the pertinent component probabilities were component unavailabilities and component failure probabilities. From the data base, the highest unavailability for a single active component is of the order of 10^{-3}. Analogously, the highest unavailability for a single passive component is of the order of 10^{-4}. Using the single failure bound, the maximum effect from common causes is thus 10^{-3} or 10^{-4}, whichever is pertinent (i.e., MIN [P(A), P(B)] equals 10^{-3} or 10^{-4}). As seen from the fault tree and event tree reports, for a number of systems the relevant system values are not impacted by even these highest potential effects of 10^{-3} or 10^{-4}.[1]

With regard to the precision of the predicted values of system failure probabilities, system values are required to only one or two orders of magnitude in accuracy for the overall risk analysis. Common mode contributions that were of the same order as the system value would therefore at maximum change the value by a factor of two or so, which was within the accuracy requirements. Furthermore, the system values already had larger error spreads due to data and modeling uncertainties. The addition of common mode contributions did not therefore impact these existing larger spreads.

There were of course exceptions in which common mode failures did impact the system values and the pertinent contributions are discussed in the fault tree reports in Appendix II.

The cases of large potential common mode impact consisted principally of failures involving human errors, environmental variations, and particular external events and failures causing or accelerating additional failures. The combination bounding technique was used in these cases to quantify a range for the probability contribution. If further investigation and analysis did not produce any more accurate information or results, the range was used as the contribution to the system failure probability.

In determining a range for the common mode probability, an upper bound and a lower bound are required to define the range. The upper bound is given by the combination bounding technique and was

---

[1] The insensitivity to common modes was also due to the fact that the system fault trees already contained single component failures. Common modes at the extreme could change multiple component failures to single component failures which already existed.

that value used in the checking. Representing an opposite end point, the lower bound gives a minimum value for the combination probability; i.e., the true combination probability is greater than the lower bound value. Where common mode failures can prevail, a lower bound on the combination probability can therefore simply be taken as the independent failure situation in which individual probabilities are simply multipled. When information existed, a better lower bound value was instead used.

With the upper and lower bound, the range is determined and can be used in the quantification analyses. The midpoint of the range, for example, can be used as a best estimate of the true probability value. Instead, the bounds themselves can be used in conservative or optimistic calculations.

In the study, since a probabilistic approach was being used, a probability distribution was associated with the range. As for the other parts of the study, a log-normal was used with its median (50% value) positioned at the center (geometric midpoint) of the range and its 90% bounds lying within the range.

In the actual determination of the log-normal distribution which was to be associated with the original range, Monte Carlo simulation was employed using the SAMPLE CODE. The reader is referred to Appendix II for details on this methodology. When there was knowledge that the true probability would lie in a particular portion of the range (for example, in the high value region), then the bounds were adjusted to incorporate this knowledge. When there was no such knowledge, then the bounds were kept as originally determined.[1]

As an example of the application of the bounding and range approach that was performed in the study, consider the miscalibration of two sets of bistable amplifiers discussed in earlier appendices. If both sets of amplifiers are miscalibrated then system failure will result. The probability for any particular set being unsafely miscalibrated is 1×10^{-3}.

Using the combination bounding technique, the upper bound for the combination failure of two sets being miscalibrated is 10^{-3} (i.e. MIN [10^{-3}, 10^{-3}]). This represents the completely dependent situation (given the first is miscalibrated, the probability is then one for the second miscalibration). The other side of the range, the lower bound, is obtained from the independent calculation, $10^{-3} \times 10^{-3} = 10^{-6}$. This represents the situation of the two miscalibration being completely independent.

When the probabilistic approach was used to incorporate the possible contributions, then the log-normal technique was used. Since there was neither strong dependence nor strong independence, the midpoint of the range was used, which is approximately

$$3 \times 10^{-5} \text{ (i.e., } \sqrt{10^{-6} \times 10^{-3}}\text{)}.$$

To cover the possible variations, the individual probabilities were treated as random variables and Monte Carlo simulation was employed for the final system quantification (section 3.6.2 of Appendix II).

3.4 MORE DETAILED QUANTIFICATION APPROACHES

This section discusses certain of the concepts and techniques which can be applied if more detailed quantification of common mode failures is necessary. In the Study, because of the results obtained, these more detailed quantifications had a minor role. An approach will be discussed here which was used as a supplemental technique for common mode quantification. It will also serve to illustrate the types of considerations which can be included in general dependency modeling.

The approach presented deals with discrete failure events, which can then be extended to the continuous time domain (incorporating time dependencies of the probabilities). Consider again the combination AB, which represents the failure of both A and B. Various mechanisms can cause AB to fail, and hence the probability of AB, P(AB), can be broken into various mechanistic contributions.

Let M denote a particular mechanism which if it were to occur could cause

[1] With regard to the log-normal, the median was thus centered at the geometric midpoint of the original range, or on geometrically subdivided regions, depending upon the relevant information.

both A and B to fail. The total probability, P(AB), can then be expressed as

$$P(AB) = \sum_{M=1}^{N} P(M)\ P(AB/M) \qquad \text{(IV 3-24)}$$

where

P(M) = the probability of mechanism M occurring

(IV 3-25)

and

P(AB/M) = the probability of AB failing when mechanism M exists

(IV 3-26)

In equation (IV 3-24), the summation symbol $\sum_{M=1}^{N}$ denotes summation over all pertinent mechanisms (say, a total of N of them). Equation (IV 3-24) is the standard decomposition of a probability into its elemental contributions (termed a mixture decomposition in probability methodology).

It is important to note in Equation (IV 3-24) that the likelihood of M, P(M), and its effect on AB, P(AB/M), enter in the form of a product, i.e., P(M)P(AB/M). Therefore, if the effect of M on AB is large but its likelihood is small then the resulting product contribution could be small. However, if the likelihood of occurrence of mechanism M is small but is of sufficient size to cause the product term to dominate, the contribution would then be significant. The summation in Equation (IV 3-24) can therefore be considered to be over those mechanisms for which the product terms dominate.

The mechanisms defined in Equation (IV 3-24) are general and incorporate the spectrum of component properties and environments which can exist. Since the summation is over all mechanisms whether they are common cause related or not, the independent, non-common cause situation can be treated as one "mechanism". This non-common mode mechanism, or environment, is within the design environment under which components fail independent. This environment will be termed the independent environment.

If the independent environment is denoted by M_O, then Equation (IV 3-24) can be broken into an independent contribution and a common cause contribution:

$$P(AB) = (PM_O)P(AB/M_O) + \sum_{M\ \text{(common cause)}} P(M)P(AB/M) \qquad \text{(IV 3-27)}$$

The last term in Equation (IV 3-27) is a summation over all mechanisms which do not lead to independence, i.e, over all common cause mechanisms.

By the definition of the independent environment M_O, the components fail independently of one another. Hence,

$$P(AB/M_O) = P(A)P(B) \qquad \text{(IV 3-28)}$$

Consider now the occurrence probability for M_O, i.e., $P(M_O)$. Under efficient design, manufacturing and quality control, and testing and maintenance, a larger portion of potential common modes are eliminated or are detected and corrected. Hence, for these cases, which are characteristic of present-day, efficient procedures, $P(M_O) \approx 1$.

The above equality, $P(M_O) \approx 1$, simply says that for a larger portion of the time and cases, say at least 50%, an approximately independent environment exists. This does not say that common cause mechanisms do not dominate the combination failures since their relative effects can be large. In fact, all combination failures which occur can be due to common causes. This is a relative effect, where the combination failures constitute the base of comparison. The equation $P(M_O) \approx 1$, concerns an absolute frequency, for example implying that the combination failure does not occur daily.

For normal environments the approximation $P(M_O) \approx 1$ is thus reasonably accurate, yielding results with reasonable accuracy.[1] (For peculiar situations where non-normal deviations are more likely, the assumption will be slightly conservative and yield conservative results.) Using $P(M_O) \approx 1$ and the

[1] The accuracy for example, is within several significant figures for failure detection efficiencies of greater than 90%, where the efficiency incorporates the efficiencies of all stages, design, manufacturing, testing, etc.

independence of A and B under M_o, Equation (IV 3-27) then becomes:

$$P(AB) = P(A)P(B) + \sum_{M \text{ (common causes)}} P(M)P(AB/M) \qquad \text{(IV 3-29)}$$

The above equation is the final form thus obtained, in which failures are decomposed into independent and common mode contributions.

Equations (IV 3-24) or (IV 3-29) can be used to quantify the total combination probability or a particular common cause contribution. The occurrence probabilities P(M) are obtained from examination of quality control processes, testing, etc., to determine their relative efficiencies. Processes can be grouped into classes for greater information utilization, thus giving larger population bases. The probabilities P(M) can be determined directly from experience data using standard estimation techniques or can be modeled using such techniques as stochastic process theory.[1]

The probabilities P(AB/M) represent failure behavior under various given environment and situations. These probabilities can be modeled using standard reliability techniques, taking into account the particular sensitivities and properties of the components involved.

If the mechanisms are extreme, then the approximation can be used that P(AB/M) $\simeq$ 1 (the mechanism is certain to cause failure). Degradation models can be employed where the mechanisms impose stress-type conditions (k factors and Arrhenius modeling are examples of such approaches).

Instead of being obtained by modeling, the probabilities P(AB/M) can also be directly obtained from experience data. This is particularly so when the mechanism causes a higher failure probability, thereby yielding some data. Even if the mechanism is corrected, the data can still be utilized for estimation, with checking and correction then separately incorporated in the model (analogous to incorporating repair in standard reliability modeling). Empirical data fitting and controlled designs can also be employed (use of the Weibull distribution is an example of the former and environmental testing of the latter).

In the quantification of Equation (IV 3-24) or (IV 3-29), the amount of detail can be adapted to the problem needs and data available. For those calculations in which order of magnitude accuracy only is desired, the analysis and required information will be greatly simplified. In certain cases, one mechanism can be isolated as yielding the dominant contribution (for example, considering the one mechanism for which the components are most failure-sensitive). Bounding and range calculations can also be performed. Flexibility therefore exists in the utilization of these equations, as will be illustrated in the application discussions of this section.

Equations (IV 3-24) and (IV 3-29) can straightforwardly be transformed to incorporate time dependencies. These time dependent forms are often the ones utilized in quantification and modeling. If the mechanism can exist at the time of component installation, i.e., at t = 0, then P(M) is a constant, initial-condition probability P(M) = P. This is applicable to design, manufacturing, and quality control defects, and also other phenomena which are inherently associated with the component.

If the mechanism is not directly tied to a component property, but instead can occur over some exposure time, then P(M) is a cumulative time-dependent distribution, or equivalently a time dependent density function. This form is applicable to testing and maintenance errors, environmental degradation, and other phenomena which occur during operation and use of the component. Applicable forms for P(M) are those associated with renewal theory or stochastic process theory for example. A common model is a Poisson process, with either time independent or time dependent occurrence rate; i.e.,

$$P(M) = 1 - e^{-\lambda t} \text{ or } P(M) = 1 - e^{-\Lambda(t)}$$

where λ and $\Lambda(t)$ are the associated parameter rates.

In time dependent analyses, failure probability P(AB/M) is treated by standard reliability techniques, with the

---

[1] For this estimation and modeling, the formulas are generally utilized in their time dependent form, as discussed later.

condition that mechanism M has occurred. The probability is thus conditional, analyzed under the environment or characteristics of the mechanism M, and the probability is in general dependent (a bivariate for example). The definitions of P(AB/M) are similar to those normally employed; for operating or standby failures, P(AB/M) is a cumulative failure probability or an unavailability, respectively. For cyclic failures, P(AB/M) can be treated as a demand probability.

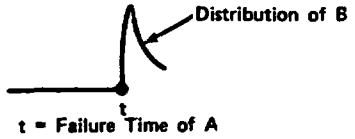
The functional forms for P(AB/M) are those used in reliability and statistical theory with, for example, parameter values chosen to correspond with the given condition of M having occurred. Exponentials, for example, can be used with modified failure rates (such as in the k-factor approaches).

The standard bivariate exponential can be used for correlated failure modeling, where the bivariate form is given by,

$$P(AB/M = \exp[-\lambda_1 t_1 - \lambda_2 t_2 - \lambda_3 \max(t_1, t_2)] \quad \text{(IV 3-30)}$$

where t_1 and t_2 are the failure times of A and B. The probability is for failure times being greater than t_1 and t_2. The parameters λ_1 and λ_2 relate to the individual failures and λ_3 to the coupled or dependent contribution.[1]

Instead of dealing directly with the combination probability P(AB/M), the individual contributions (marginal distributions) can also be analyzed. In terms of the individual probabilities, P(AB/M) = P(A)P(B/A), where the given condition of M is implicit in each probability on the right hand side. A straightforward approach is, for example, to use an exponential distribution for P(A) with an appropriate failure rate and a truncated normal or exponential for P(B/A) located at the failure time of A. A heuristic diagram of this model is shown below.



As illustrated, given A has failed, B is no longer independent but has a high probability of failing at or near the time of the A failure. In the extreme case, the distribution of B becomes a delta function. The equations for this model and other coupled, conditional models are obtained from conditional probabilistic theory.

The techniques that have been briefly outlined above are by no means exhaustive, but they help in circumscribing the various possible approaches. Since the approaches are varied, each individual problem must be evaluated to determine the specific approach which is applicable, and also compatible with the available data. The approaches are all straightforward and involve standard statistical and reliability techniques, utilizing either gross data or detailed data.

Upper bounds can be obtained from Equations (IV 3-24) and (IV 3-29) by using conservative values for P(M) and P(AB/M). Lower bounds can be obtained by using associated lower bounds for these terms or by neglecting contributions in the summation [for example, using only the independent contribution in Equation (IV 3-29)].

The above bounding approaches can, for example, be applied to common mode failures that can be due to external events or previous failures having occurred. As a specific illustration consider the common mode failure due to a steam line rupture which was investigated in the study.

For the steam line rupture mechanism, using Equation (IV 3-29), P(M) is then the probability that the steam line rutpures, and P(AB/M) is the probability that the nearby components (control circuits, etc.) are failed by this occurrence. An upper bound for this contribution can be obtained by using a conservative estimate for the steam line rupture P(M) and a conservative estimate for the affected failure probability P(AB/M).

A straightforward approach for P(AB/M) is to use the fraction of solid angle subtended by the pertinent components (i.e., fraction of area exposed) or to assume P(AB/M) = 1. For the steam line rupture P(AB/M) = 1 was used and the solid angle approach was used for those cases involving missile-type generation, e.g., turbine runaways [for the missile investigations P(M) = probability of turbine runaway, P(AB/M) = critical fractional solid angle].

---

[1] If the failures were independent, then $\lambda_3 = 0$, giving simply a product of exponentials as in the random failure approach. For $\lambda_3 \neq 0$, the failure times are coupled.

Using $P(AB/M) = 1$ for the steam line rupture case, Equation (IV 3-29) becomes,

$$P(AB) < P(A)P(B) + P(M) \qquad \text{(IV 3-31)}$$

From the Study's data base an upper bound for $P(M)$ is 10^{-7}, when a conservative, leak type failure rate is used and a 1 hour window exists about the accident time. Hence, to order of magnitude

$$P(AB) < P(A)P(B) + 10^{-7} \qquad \text{(IV 3-32)}$$

For these cases then, if the independent probability $P(A)P(B)$ is greater than 10^{-7}, the common mode contribution is negligible. If the independent probability is less than 10^{-7}, then 10^{-7} can be used as the upper bound, for example, in assigning the log-normal probability range for $P(AB)$ (the lower bound of the range consisting of the independent contribution). Equation (IV 3-32) and the bounds are applicable to any combination AB which were encountered in the fault trees (constituting a critical path) and which were located adjacent to a steam line.[1]

---

[1] Further detailed descriptions of this type of analyses are given in the special engineering investigations to be discussed.

TABLE IV 3-1 CLASSES OF POTENTIAL COMMON MODE MECHANISMS

A. Design Defects
B. Fabrication, Manufacturing, and Quality Control Variations
C. Test, Maintenance, and Repair Errors
D. Human Errors
E. Environmental Variations (Contamination, Temperature, etc.)
F. Failure or Degradation Due to an Initiating Failure
G. External Initiations of Failure

TABLE IV 3-2 COMBINATION PROPERTIES INDICATING POTENTIAL COMMON CAUSE SUSCEPTIBILITY

1. All Components Identical in Type and Specification (A,B)
2. Components All Under the Same Maintenance or Test (C)
3. All Components Having Similar Failure Sensitivity (E,G)
4. Components All in the Same Locations (E,F,G)
5. Components All Exposed to a Possible Accident Environment (E)
6. All Components Loaded or Degraded by a Previous Failure (F)
7. All Component Failures Human Initiated (D)

Section 4

Failure Coupling

Because of common quality control, common manufacturing processes, common design, or common influencing environment, components can be coupled in a different type of common mode manner. One form of this coupling manifests itself in the failure rates of the components. The specific result is that affected components will all have higher failure rates than normal. In certain beneficial situations, the affected components can also all have lower failure rates as compared to the normal values for those components.

A particular example of failure rate coupling is the existence of a manufacturing/manufacturing defect in a group of relays. Because of the defect all relays in the produced batch will thus be affected. This effect will manifest itself in all the failure rates being higher than the average failure rate for that type of relay.

Instead of a detrimental effect, the failure rates may all be lower than their standard value. Such an effect will occur, for example, if better than average maintenance is being performed on a set of components. Whether the effect is detrimental or beneficial, a coupling occurs in the affected components thus causing a certain loss of independence.

As a numerical illustration of the failure rate coupling effect, assume two latching relays are in parallel (i.e., a double failure is needed for system failure). For this type of relay, assume the normal failure rate is 10^{-3} per demand. If normal situations existed, the probability for both independently failing is then $10^{-3} \times 10^{-3} = 10^{-6}$. For the two particular relays, however, because of a coupling defect assume that both failure rates are now 10^{-2}. The joint probability given this defect, is therefore $10^{-2} \times 10^{-2} = 10^{-4}$. The failure rate coupling consequently yields two orders of magnitude increase in the joint probability of failure.

The above example yields a two order of magnitude effect given that the defect does indeed exist. A quantitative treatment must also incorporate the probability of the defect first existing. In the Study, to investigate the effects of failure rate coupling in a probabilistic manner, the failure rate distributions were coupled in a one to one correspondence.

In the normal calculations (representing no failure rate coupling), each component failure rate in the Study was assigned a distribution to account for individual variations and uncertainties.[1] The distributions were then propagated to obtain the possible variation on the resultant system failure probability. The possible system variation is represented by confidence spreads (probability ranges) on the system probability. In the normal calculations, all component failure rate distributions were treated as being independent of one another.

In the failure-rate coupling analyses, the same failure rate distributions were used for the normal calculations. Components were however, now categorized into characteristic classes where the characteristic classes were defined such that all components in a particular class had a potential common coupling cause. A characteristic class thus represented a potentially coupled set.

In the Monte Carlo simulation, components of one characteristic class were coupled by equating the component failure rates to a common single failure rate. An example of the failure rate coupled model used in the study is shown in Fig. IV 4-1. The components are of the same characteristic class, for example two similar relays. Each of the curves in Fig. IV 4-1 represents the distribution of the individual failure rate (i.e., its density function). In the independent case, when one failure rate is low (the above figure), the other failure rate can be high (lower figure). This independent behavior represents the independent individual component variations which can occur.

In the coupled case, when one failure rate is high, the other failure rate in the same coupled class is also high. In

---

[1] See Appendix II.

complete coupling, as is shown, all components have the same failure rate (one to one correlation).[1] In this coupled treatment, the probability of the coupled variation existing is incorporated by the individual component failure rate distribution (the upper curve in the coupled case). (Given a particular failure rate value (the "x" sampled on a curve) the coupling is then established by assigning the same failure rate value to all the other components of the same characteristic class.)

In the Study, the characteristic classes of components coupled were defined to be components of the same basic functional type. All relays constituted one class, all pumps another, motor valves, wires, etc., other classes. This categorization corresponded to the general categorization breakdown in the failure rate data base (Appendix III). The establishment of these characteristic classes enabled the examination of a very broad range of potential couplings to be made. In general, many people have thought of such potential couplings as including only components that were quite specifically related such as relays, pumps, valves, etc. of a given manufacturer. Since the classes used herein were much broader, the coupling studies performed included <u>all</u> generally similar components such as all relays, all pumps etc. within a particular system.

Since the test and maintenance downtime represents a unique, non-component contribution to the system probability, no coupling was assigned to it. The test and maintenance downtime was thus treated as in the independent case. Common mode human errors are explicitly incorporated as separate contributions to the system probability. Therefore, the human contributions were also not failure rate coupled (human contributions were thus also treated as in the standard independent case). The coupled classes were consequently those composed only of hardware failures.

In the study, the coupled variation was evaluated by Monte Carlo sampling using the SAMPLE program (described in Appendix II). Sampling a failure rate value from an individual distribution gave all the failure rates for that class. The coupling was repeated in this sampling manner to obtain the resultant variation in the system probability. (A more detailed description of the actual sampling procedure is given in section 3.6.2 of Appendix II.)

The coupled modeling which was used had the effect of increasing the error spread of the system probability. The distribution and associated error spreads on the system probability then represented the possible variations including the common mode coupling effects. The system error spreads thus became larger, as compared to the normal independent calculations, accounting for the coupling effects. The amount of widening, as compared to the independent case, represents one measure of the effect of coupling existing in the system. The coupling effect is illustrated in Fig. IV 4-2.

It should be noted that the model described is simply one method of coupled treatment. It is applicable when coupling effects are incorporated into the system distribution. More detailed models can be employed by which the coupling effects are incorporated into the actual system probability value. This requires a more detailed type of data, but is useful when, for example, higher accuracy is required.

Table IV 4-1 shows the results of studies that were performed to determine the effect of common mode coupling on the PWR and BWR system probability bounds, using the modeling techniques previously discussed. The independent 90% bounds were those obtained by the standard, independent treatment. The coupled 90% bounds were those obtained by completely coupling all the generic classes. In general the error bands became larger for the dependent case and the median only slightly changing. The results listed in the table are those for which the coupling had some observable effects. Even for these cases, the coupling effect is not an order of magnitude significance and does not have a very large impact.[1] As extra error

---

[1] In a statistical methodology the one to one correlation is represented by equating the random variable failure rates, $\lambda_1 = \lambda_2 = \lambda_3$, etc.

[1] In general, the coupling has greater effect in systems having dominant failure contributions from single characteristic classes. The coupling effect is therefore useful for general investigations of component diversity within systems. The smaller effect in the study's results was due to the systems being dominated by single failure and non-hardware contributions (test and maintenance, human).

coverage, however, the coupled values were used in the fault tree reports for those systems where the relative effect was larger and could impact further evaluations. (This also gave added protection against biases and correlations resulting from non-independent estimation of the component data.)

TABLE IV 4-1 PWR COUPLING - BWR COUPLING

System	Case	Lower Bound	Median	Upper Bound
		PWR COUPLING		
RPS	Independent	1.3×10^{-5}	3.6×10^{-5}	1.0×10^{-4}
	Dependent	8.4×10^{-6}	3.0×10^{-5}	4.3×10^{-4}
LPRS	Independent	4.4×10^{-3}	1.3×10^{-2}	3.1×10^{-2}
	Dependent	2.1×10^{-3}	9.6×10^{-3}	6.5×10^{-2}
HPRS	Independent	4.3×10^{-3}	9.0×10^{-3}	2.2×10^{-2}
	Dependent	2.1×10^{-3}	9.0×10^{-3}	4.0×10^{-2}
HPIS	Independent	4.4×10^{-3}	8.6×10^{-3}	2.7×10^{-2}
	Dependent	2.4×10^{-3}	1.8×10^{-2}	5.0×10^{-2}
AFWS SPB(Start & 8 Hrs.)	Independent	7.0×10^{-6}	3.7×10^{-5}	3.0×10^{-4}
	Dependent	4.2×10^{-6}	3.2×10^{-5}	6.0×10^{-4}
		BWR COUPLING		
ECI - I	Independent	1.0×10^{-3}	1.5×10^{-3}	2.1×10^{-3}
	Dependent	9.4×10^{-4}	1.5×10^{-3}	3.6×10^{-3}
ECI - II	Independent	1.0×10^{-4}	2.0×10^{-4}	3.0×10^{-4}
	Dependent	8.2×10^{-5}	2.0×10^{-4}	5.0×10^{-4}
ECI - III	Independent	8.4×10^{-8}	9.3×10^{-7}	1.0×10^{-5}
	Dependent	6.3×10^{-8}	8.6×10^{-7}	4.2×10^{-5}
RPS	Independent	4.3×10^{-6}	1.3×10^{-5}	4.8×10^{-5}
	Dependent	2.3×10^{-6}	1.3×10^{-5}	8.9×10^{-5}
CSIS (Both Legs)	Independent	6.7×10^{-4}	9.5×10^{-4}	1.4×10^{-3}
	Dependent	4.5×10^{-4}	9.5×10^{-4}	2.6×10^{-3}

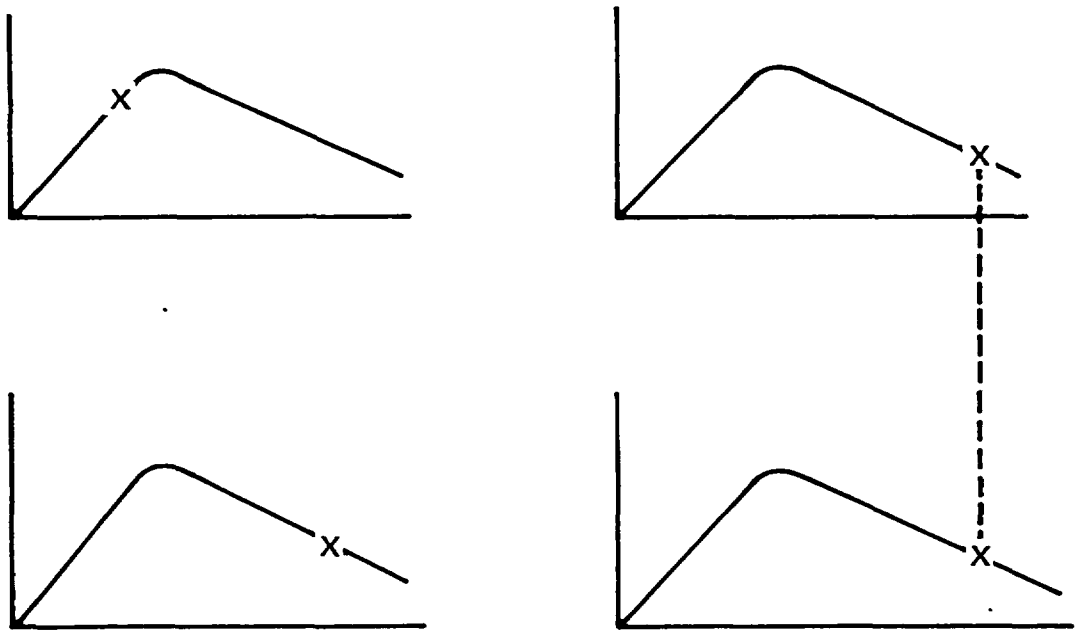


FIGURE IV 4-1 Independent Versus Coupled Failure Rate Distributions [Frequency on Vertical Axis (Ordinate), Failure Rate on Horizontal (Abscissa)]

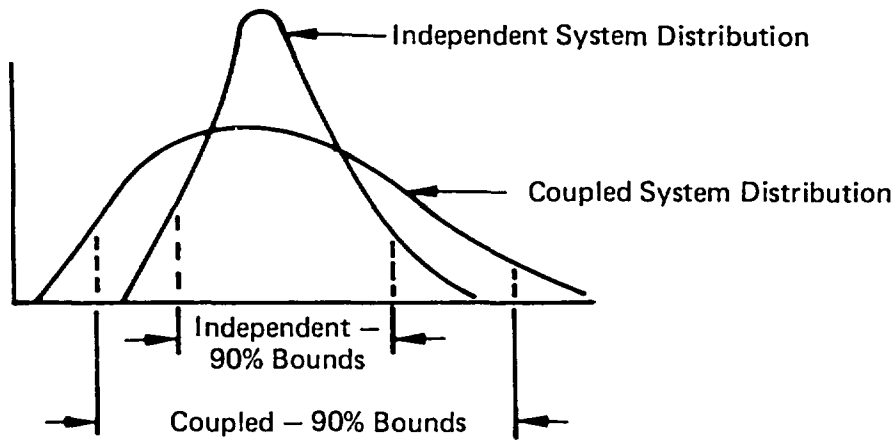


FIGURE IV 4-2 Increased System Uncertainties Due to Coupling Effects (Vertical Axis - Frequency; Horizontal - System Probability)

Fig. IV 4-1 — Fig. IV 4-2

Section 5

Special Engineering Studies to Identify Potential Common Modes in Accident Sequences

5.1 SUMMARY OF RESULTS

In this special engineering study, common mode failures are again examined for their possible contribution to PWR accident sequence failure probabilities. From these engineering studies, it was found that the common mode failure probabilities in general did not significantly impact these failure probabilities.

Many of the accident sequence failure probabilities are dominated by component failures in subsystems that have interfaces with more than one system in a sequence or by common human errors that affected redundant systems. These are failures, however, which were identified and evaluated in the individual system fault analyses,[1] and were previously taken into account when the systems were considered together in the evaluation of the accident sequence probabilities.[2] This common mode failure study therefore did not include the already considered multi-system sequence failures due to individual component failures in interfacing subsystems, or the human interface, acting through a common human error, failing redundant legs of a system.

Two types of common mode failures were examined in this special study:

a. Common mode failures from secondary failure sources, are component failures resulting from phenomena, such as flooding or fire, which exceed component design limits. This type of common mode includes failures in one system which can indirectly fail the other systems in the sequence. In some cases, the secondary failure sources may cause multiple system failures through a common interface.

b. Common mode failures in similar components are failures involving several similar components (such as motor-operated valves or motor starter breakers) used in more than one system where the components can all fail within a critical time frame due to some common cause (such as a manufacturing error).

5.1.1 LARGE LOCA SEQUENCES

In addition to the above, the potential for common mode caused damage to safety systems and to the containment structure due to whipping motions of ruptures RCS piping was considered. ("Pipe whip" is a term commonly given to this type damage potential.) In this consideration, the layouts of the reactor coolant system (RCS) and other high energy piping relating to the preservation of containment integrity and the safety systems piping runs were examined. Restraints to prevent potential pipe whip were found to be applied where the possibility of interaction between a ruptured pipe and containment might potentially occur (e.g. main steam and feedwater lines[1]). No pipe whip damage mechanisms were identified in the case of safety systems since, in all areas considered, the presence of the crane wall and operating decks provided adequate protection. In these cases where individual legs of emergency cooling (ECCS) piping ran from the crane wall to the RCS connections, the loss of function for that ECCS leg was assumed to occur whenever that part of the RCS loop ruptured. This common mode failure of the ECCS connection to a single RCS loop was incorporated in the analysis of ECCS overall failure probability as stated in Appendix I, section 2.4 and in Appendix II, section 5.6.

The accident sequences in the Large LOCA event tree which were investigated for these types of failures were chosen because they had some potential susceptibility for common modes and their probability could have been affected if

---

[1] See Appendix II for system fault analysis descriptions.

[2] See Appendix I for event tree discussions, and Appendix V for sequence evaluations.

---

[1] See Appendix X, subappendix A, section A6.3.2.

such common modes existed. The symbols used in the subsequent discussions are as follows:

A = Large LOCA (loss-of-coolant accident);

B = EP (Electric Power);

C = CSIS (Containment Spray Injection System fails);

D = ECI (Emergency Cooling Injection failure, which is essentially the failure of the LPIS, or Low Pressure Injection System, for a large LOCA);

F = CSRS (Containment Spray Recirculation Systems fails);

G = CHRS (Containment Heat Removal System failure);

H = ECRS (Emergency Cooling Recirculation System failure, the failure of the LPRS, or Low Pressure Recirculation System, for a large LOCA);

I = SHAS (Sodium Hydroxide Addition System failure, the system to supply NaOH to the containment and the containment sump by injection into the RWST).

The sequences for which the common mode failures were evaluated, and the results of the evaluation, are as follows:

Sequence[1]	Common Mode Impact
CD	Insignificant
CDI	Insignificant
HF	Minor Impact
G	Insignificant
D	Within Error Spreads
CF	Insignificant
B	Insignificant
F	Insignificant
HFI, HI, FI	Insignificant

The sequences HF (given A) and D (given A) were identified as having some potential for non-negligible effects, but even for these cases the impact on the probability of the release category was assessed to be small and within the error spreads.

[1]See the PWR event tree discussion in Appendix I for discussion of the detailed meaning of these sequences.

The HF (given A) sequence has as a contributor the common mode failure of the containment sump. The blowdown during a LOCA causes an accumulation of debris in the containment which in turn plugs the sump, with a value on the probability of plugging the sump of 10^{-6}[10].[1]

The D (given A) sequence had as a contributor a common mode failure in which a LOCA on the discharge side of the primary coolant pump causes pump overspeed and flywheel fracture. A piece of the fractured flywheel penetrates the cubicle wall in the vicinity of a single pipe for low pressure injection to the cold legs, thereby striking and failing this line (therefore failing D). This event sequence had a probability of approximately:

$$Q_{CM} \approx 1.3 \times 10^{-6}$$

5.1.2 SMALL LOCA SEQUENCES

Small LOCA event sequences involve most of the same systems and event codes as the large LOCA events, except for the following:

S = Small LOCA;

D = ECI (essentially the failure of the HPIS, or High Pressure Injection System);

H = ECR (the failure of the HPRS, or High Pressure Recirculation System);

K = RPS (failure of the Reactor Protection System);

L = AFWS and SSR (failure of the Auxiliary Feedwater System and Secondary Steam Relief valves).

The results of the evaluation for the contribution of common mode failures to small LOCA event sequences are in general the same as for the large LOCA event sequences; that is, the common mode contributors have probabilities which do not significantly impact the sequence failure probability or the release category probability.

The D (given S) sequence does not include the common mode contributor of

[1]Quantity within the brackets is the error factor which applies.

the flywheel failure (pump B flywheel failure), because the relatively slow depressurization of the reactor coolant system (RCS) will not cause pump overspeed. Other sequence common mode failures (primarily a RCS stop valve failing closed causing a severe water hammer and a LOCA) have probabilities that are orders of magnitude less than the independent unavailability of D (the HPIS).

The small LOCA sequences involving the K and L systems are not among the important contributing sequences for small LOCA events. Since no significant common mode failures were determined for K or L that affect other systems in the sequences (common mode failures involving only K or L systems were developed and evaluated as a part of the analysis for those systems[1]), common mode failures for those small LOCA sequences involving K and L systems will not be discussed further.

The C (given S) sequence is an important small LOCA sequence for the S2 LOCA (a small LOCA due to a break in the RCS equivalent to a hole with a 1/2 to 2 inch diameter). However, no significant common mode failures could be found for the CSIS, other than common human errors already considered as a part of the CSIS fault analysis.[2]

These considerations leave the HF (given S) sequence as the important small LOCA sequence with a common mode failure between systems of the containment sump plugging failure. Even though the probability of the sequence is affected, the impact on the release category is, however, insignificant and within the error spreads of the release category probability.

5.2 SUMMARY OF SECONDARY FAILURE METHODS

Secondary failure sources were identified in studies of plant layout, and of potential interactions between system components and between energy sources and system components. Plant drawings and visits to the plant were used for this study. A summary of the influence of the secondary failure sources on the sequences being evaluated is in subsection 5.4.2. A summary of common faces through which common mode failures may fail PWR LOCA sequences is in subsection 5.4.1.

A list was compiled from the system fault trees, system drawings, component specifications, and other plant design information listing similar components used in the PWR Safety Systems which can fail a system or multiple systems by the failure of several similar components in a given failure mode within a critical time frame. The listing, and the PWR LOCA sequences which can be affected by multiple failures of similar components are presented in Table IV 5-1.

5.3 PWR LOCA SEQUENCE COMMON MODE FAILURE EVALUATIONS

The more detailed evaluation of the potential common mode failures for the PWR LOCA sequences summarized earlier is given below. The single letter codes used to identify PWR systems are listed in the preceeding section 5.1. The evaluation discussion below does not include those common mode failure contributors which were found to have a negligible influence on the total common mode failure contribution.

5.3.1 SEQUENCE CD (GIVEN A OR S)

Common mode contributors are not significant contributors to the CD sequence failure probability, since their probability was one to two orders of magnitude less than for the CD sequence as determined from the basic fault trees. A common mode contributor for the CD sequence is the event of four or more 480 V motor starter breakers for the system pumps could all trip due to a common cause. The probability for this common mode contribution was assessed to be much less than the CD sequence failure probability already evaluated.

5.3.2 SEQUENCE CDI (GIVEN A OR S)

The CDI sequence failure probability has as a contribution failure of the RWST common interface, primarily by plugging of the 8 inch RWST vent. This probability was assessed to be comparable to that of passive component failures for the LPIS system[1].

---

[1] See Appendix II, section 5.2 for the RPS, section 5.3 for the AFWS.

[2] See the CSIS analysis in section 5.4 of Appendix II.

[1] See section 5.6.3 in Appendix II for the LPIS analysis.

CDI sequence common mode contributors (interacting with the sequence by failing the RWST) do not significantly add to the CDI sequence failure probability, as follows:

a. Rupture of the RWST by an exploding high pressure gas bottle in the adjacent bottle farm.

b. Rupture of the RWST by a vehicle crashing into the RWST. This was the dominant common mode failure. The probability of this event, however, was insignificant compared with the CDI sequence failure probability.

Common mode failure of the Safety Injection Control System (which fails D) coupled with failures of the CI sequence also can contribute to common mode failures for the CDI sequence. These failure combinations are again assessed not to be significant contributors.

5.3.3 SEQUENCE HF (GIVEN A OR S)

The possible common mode contributor for the HF sequence is:

Plugging of the containment sump after a LOCA is assessed as 10^{-6}[10]. This contribution is included in the event sequence probability; however, the effect on the total release category probability is small.[1]

5.3.4 SEQUENCE G (GIVEN A OR S)

The G(CHRS) sequence failure probability for the first day of recirculation has as a contribution the drainage of the intake canal, an interfacing system. A human interface common mode failure, previously developed and evaluated in the CHRS fault tree analysis,[2] is the failure of operators to open the containment heat exchanger vent valves, which leads to air entrapment in heat exchangers when flow is initiated and failure of the heat exchanger function.

Other identified common mode contributors which were assessed to have insignificant contribution to the G sequence failure probability are:

a. A rupture of the turbine oil conditioner spilling oil into the adjacent service water valve pit. If this oil is ignited, the normally closed motor operated valves (MOV's) in the valve pit for service water to the containment heat exchangers may be failed.

b. Two check valves fail to open on demand due to a common failure cause.

c. Rupture of a service water line in the service water valve pit floods containment heat exchanger MOV's, preventing their opening for a LOCA.

d. Four MOV's inadvertently closed within 24 hours.

e. Two bellows joints rupture within 24 hours.

5.3.5 SEQUENCE AD (GIVEN A)

Identified common mode contributors could affect the AD sequence failure probability; however, the impact is still within the error spread.

A possible common mode contributor for the AD sequence has a probability which could at most double the probability for independent A and D events. This common mode failure is a rupture (LOCA) in the RCS piping at the discharge side of RCS pump B which would cause the pump to overspeed and potentially result in a flywheel fracture. A piece of the fractured flywheel penetrates the loop B cubicle wall near the single line for low pressure injection to the cold legs, and ruptures this line thus failing the LPIS (D). The common mode failure was conservatively evaluated as follows:

$$Q_{CM} = Q_{LOCA}\, Q_{BD/L}\, Q_{PF/B_b}\, Q_{TA}$$

Q_{LOCA} = The probability of a large LOCA = 1×10^{-4}/yr.

---

[1] Consideration of the overall probability results for core melt (see Table V 3-14, Appendix V) also indicates that the results are not particularly sensitive to large variations in the probability estimates for containment sump plugging. For example, an increase of two orders of magnitude in the HF sequence due to the sump plugging contribution still has small effect.

[2] See section 5.6.3 in Appendix II for the LPIS analysis.

$Q_{BD/L}$ = The probability of a rupture in the pump B discharge line ≃ .13[1]

$Q_{PF/BD}$ = The probability of flywheel fracture ≈ 1.0[2]

Q_{TA} = The fraction of the susceptible circumferential area around pump B ≅ .1

Q_{CM} ≈ (1×10^{-4}) (.13) (1.0) (.1) = 1.3×10^{-6}, which would be approximately double the probability for independent A and D events. The value is, however, within the error spreads.

Regarding the AD sequence, another identified potential common mode failure results if one of the six RCS stop valves fails, allowing the valve disc to drop and suddenly stop loop flow. The sudden flow stoppage could cause an excessive water hammer which ruptures several emergency core-cooling system (ECCS) piping connections to the RCS in more than one of the loops, resulting in a LOCA and failure of several ECCS systems. Essential ECCS piping would be lost if 2 out of 3 accumulator lines were ruptured, or if 3 out of 3 LPIS lines to the cold legs were ruptured. This common mode failure was assessed to have a probability less than the pump flywheel failure.

5.3.6 SEQUENCE CF (GIVEN A OR S)

The CF sequence failure probability is dominated by failure of the consequence limiting system (CLCS), a common interfacing system with the CSIS and CSRS. Failure of the CLCS is in turn dominated by a human common mode failure, miscalibration of CLCS instrumentation. This common mode failure was developed and evaluated in the CLCS fault tree analysis.[1]

The CLCS, and the CSIS and CSRS may also be failed due to common mode failures of similar components. An evaluation for these failures found them not to impact the CF sequence failure probability. These similar component common mode failures (not including human calibration errors) are:

a. Three CLCS Hi-Hi relays fail to energize.

b. Three containment pressure transducers fail to respond to low pressure.

c. Three power supplies have low voltage.

d. Three signal comparators drift up.

e. Six 480 V motor-starter breakers fail to close.

f. A fire in the instrument room fails both trains of the CLCS.

g. Four MOV's inadvertently closed.

h. Six 480 V motor-starter breakers trip.

5.3.7 SEQUENCE B (GIVEN A OR S)

Possible common mode contributors for EP failure are determined not to impact the EP failure probability.

These common mode contributors, for the B sequence are:

a. The electrical switchgear overheats and fails when switchgear room air conditioning is lost due to an explosive failure of one of the three air conditioning chiller air compressors which fails adjacent chillers, or fails the service water supply to the chillers, or fails the power to the chillers.

b. The switchgear overheats and fails when air conditioning is lost due to explosions of high pressure air bottles in Mechanical Equipment Room No. 3 failing the service water supply to the air conditioning chillers or severing the power cables for the chillers.

---

[1] 40% of the RCS loop piping is on the discharge side of the pumps and there are 3 loops; so $Q_{BD/L}$ = .4/3 = .13.

[2] The value used for $Q_{PF/BD}$ is considered somewhat conservative since the pump overspeeds attained may not be great enough to cause flywheel missiles to be generated. As can be inferred from Table V 3-14, Appendix V and from the above result, use of this potential conservatism still had no significant effect on the resulting overall probabilities of a core melt.

[1] See section 5.5 of Appendix II for the CLCS analysis.

c. The electrical switchgear is flooded when one of 8 condenser inlet lines ruptures and quickly floods the turbine rooms and the adjacent switchgear room.

The aforementioned three common mode failure sequences require a lower probability passive failure as an initiating event. The probability of the initiating event in combination with the short time window for the failure sequences to cause significant problems in responding to an accident (about 24 hours) results in probabilities for the common mode failures that are less than the EP failure probability determined from the fault tree analyses.[1]

Other common mode failures were evaluated but were also found to be insignificant. These were common mode failures of similar components in switchgear and motor control centers which could fail electrical power, by failing those combinations of buses defined in the electrical power failure analysis.

5.3.8 SEQUENCE F (GIVEN A OR S)

The identified common mode contributors are assessed not to be a significant contributor to the F sequence failure probability as evaluated in the CSRS failure analysis given in the fault tree reports.[2] The identified common mode contributors for the F (CSRS) sequence are common mode failures of similar components. These failures are:

a. Two MOV's inadvertently closed.

b. Four 480 V Motor-starter fail to start. This is the dominant common mode failure of these three failures.

c. Four 480 V Motor-starter breakers trip.

5.3.9 SEQUENCE HI, FI, OR HFI (GIVEN A OR S)

Since the injection of NaOH (I) into the RCS is not a critical requirement for safety system operations after a LOCA within the first days of operation, and since NaOH can be delivered via the CSIS, LPIS, or HPIS, no significant and impacting common mode failures were found to exist for these 3 sequences (HI, FI, or HFI) for the first day of recirculation.

Long term failure of I(NaOH) or I and F(CSRS) has also been previously assessed as having a negligible probability because of the several possibilities for operator action to deliver NaOH to the RCS after a LOCA. But, if NaOH is not delivered to the RCS, and if the operators are aware that NaOH is not delivered to the RCS, then the long term failure of NaOH can lead to stress corrosion in the ECR and CSR systems, due to an expected buildup of chlorides in the containment sump water following a large LOCA. Therefore, the long term failure probabilities for the HI, FI, and HFI sequences all have a common mode contributor equivalent to the long term failure probability of NaOH (I), through the above common mode failure interaction. This failure sequence requires undetected NaOH delivery failures [contributed by failure of an operator to open chemical addition tank (SHAS) block valves after a CSIS flow test], and failure of the chemical addition tank level instrumentation or failure of the operators to detect the lack of low level in the chemical addition tank, therefore, failing to detect that NaOH was not delivered to the RCS.

This common mode event is assessed not to be an impacting contributor to long term recirculation failure probabilities for the HI, FI, or HFI sequences because of the dominance of system component failures (primarily pumps).[1]

5.3.10 SEQUENCE HG (GIVEN S)

This sequence, like the G sequence, has as a contribution the drainage of the intake canal, since successful operation of both the CHRS and HPRS requires service water for cooling.

Other identified common mode contributors do not significantly contribute to the GH (given S) sequence failure probability.

5.3.11 SEQUENCE D (GIVEN S)

This sequence can occur due to failure of an RCS stop-valve disk, which is a common mode failure as described for the AD sequence. The probability of this

---

[1]See section 5.1 of Appendix II for the PWR electrical power failure analysis.

[2]See section 5.7 of Appendix II.

[1]See Appendix II.

event is evaluated to be less than the probability determined from the basic fault trees.

A number of possible common mode failures were identified for the HPIS(D), but they required a low probability passive failure as an initiating event (such as a high energy pipe rupture or an explosive pump failure). Therefore, these common mode failures did not result in an impact of the HPIS(D) unavailability.

This conclusion also applies to the HPRS(H), since the same components are used in a slightly different configuration.

5.4 SUPPORTING MATERIAL

5.4.1 SUMMARY OF THE RESULTS OF EXAMINING INTER-SYSTEM INTERFACES FOR SEQUENCE FAILURE POSSIBILITIES

Interfaces, such as common systems, common components, or the human operation interface, were examined to determine the combinations of systems and corresponding sequences which would be affected by the interface failure. The Table IV 5-2 list summarizes the results of this interface examination.

The electrical interfaces were found to not fail any of the sequences other than B (electrical power failure) since any of the combinations of the redundant emergency buses fails systems which are given to have succeeded in the sequences.

An exception is failure of the motor control centers 1H1-1 and 1J1-1, which would only fail the HPIS and HPRS. These systems, however, are not required for a large LOCA. The electrical bus interfaces for the PWR systems are shown in the Table IV 5-3.

5.4.2 SUMMARY OF PLANT LAYOUT EXAMINATION FOR SEQUENCE SECONDARY COMMON MODE FAILURES

a. Sequence - F
Secondary Failure: Containment sump plugs.

b. Sequence - F (CSRS only)
Secondary Failure: If a high probability exists for inside CSRS pump failures in a steam environment, then only one CSRS system need be failed for system failure in the first day after a LOCA, or 2 CSRS systems after that. This has already been included in the CSRS analysis.

c. Sequences - CD or CDI
Secondary Failure: LPIS pump B has a catastropic failure in which a high energy missile punches through the pump B cubicle wall failing the power cables to LPIS pump A and the CSIS motor operated valves (MOV's). Power to LPRS suction MOV's could also be failed. This would have to occur within roughly a minute to fail the CSIS (by not allowing CSIS MOV's to open).

d. Sequence - AD
Secondary Failure: A LOCA at the discharge of RCS pump B causes pump overspeed and a fracture of the pump flywheel. A fractured flywheel missile punches through the loop B cubicle wall and fails the single pipe or LPI to the cold legs.

e. Sequence - AD or ADH
Secondary Failure: An RCS loop stop valve disk falls into the closed position. The sudden flow stoppage causes a large water hammer which fails several ECCS piping connections to the RCS in more than 1 loop. Failure of the ECCS piping connections is also a LOCA.

f. Sequence - B (EP)
Secondary Failure: Switchgear room air conditioning is failed by:

1. Catastropic failure of chiller air compressor which fails an adjacent unit, or service water supply lines, or power cables.

2. Catastropic failure of high pressure dry air bottles in Mechanical Equipment Room No. 3 fails the service water supply or chiller power cables.

g. Sequence - B (EP)
Secondary Failure: Flood the switchgear room by:

1. The service water supply into Mechanical Equipment Room No. 3 ruptures and floods switchgear in the adjacent switchgear room.

2. Rupture of a condenser inlet line, floods the turbine room and the adjacent switchgear room.

h. Sequence - G
Secondary Failure: A pipe ruptures in the service water valve pit and fails CHRS MOV's before they have opened.

i. Sequence - G
Secondary Failure: Spilled oil from a rupture of the turbine lubricating oil conditioner, next to the service water valve pit, is ignited causing burning oil to spill into the service water valve pit and fail CHRS MOV's before they have opened.

j. Sequence - G
Secondary Failure: A small rupture in a condenser inlet line, or a rupture that is quickly stopped, floods the service water valve pit, nearby, before CHRS MOV's have opened.

k. Sequence - CDI
Secondary Failure: The RWST is ruptured by:

1. High pressure gas bottles in the bottle farm next to the RWST explode.

2. A vehicle crashes into the RWST, which is near the parking lot and the truck gate.

l. Sequence - CDI or CF(G,I)
Secondary Failure: A fire in the instrument room fails the safety injection control system (SICS) or the consequence limiting control system (CLCS) (SICS cabinets are next to each other, as are the CLCS cabinets).

m. Sequence - HFI
Secondary Failure: Failure to get NaOH into the RCS causes chloride stress corrosion in ECR & CSR systems, failing the piping.

n. Sequence - D (given S) or H (given S)
Many common mode failures which can fail the HPIS or HPRS were identified. These failures, requiring passive initiating events, are not likely to be significant contributors to HPIS or HPRS unavailability.

A high energy missile from a failed CSIS or AFWS pump could penetrate the concrete floor and fail HPIS and/or HPRS suction piping below the floor. Missiles from one failed charging pump could fail HPIS suction.

Rupture of a steam generator blowdown line can fail HPIS discharge MOV's at the boron injection tank, or a whipping blowdown line can fail the normal charging line to containment and fail the HPIS isolation MOV's for this line. Continued steam discharge through the ruptured blowdown line can result in an environmental failure of the charging pumps, thus failing the HPIS or HPRS.

A rupture of one charging pump service water pipe in Mechanical Equipment Room 3 can flood and fail the pump in the redundant charging pump service water pipe, below. This failure would fail the HPIS or the HPRS.

Secondary failure number 6, above, will also fail the HPIS or HPRS by failing the service water supply to the charging pumps.

5.4.3 SYSTEMS WHICH CAN BE FAILED BY COMMON MODE FAILURE OF SIMILAR COMPONENT

Table IV 5-1 shows the results of an examination of PWR safety systems for similar components which can fail a system or several systems if they fail by a given failure mode within a critical time frame by some common mode failure. This type of failure would be most likely due to manufacturing, design, or installation errors. The numbers in the table under the sequence codes designate the minimum number of the similar components which must fail to cause the sequence failure. The effects of these failures were evaluated to not impact the previously obtained probability.

TABLE IV 5-1 SIMILAR COMPONENT FAILURES AND SIGNIFICANT AFFECTED SEQUENCES (LARGE LOCA)

Component Type	Failure Modes	Affected Sequences							
MOV	Fails to open	CH 6	CHI 8	CG 8	CHG 10	CGI 10	CHGI 12	CD[b] 6	CDI[b] 8
	Closes	H 2 FI 4 CH 4 CD 3	HI 4 HFI 6 CHI 6 CDI 5	G 4 D 1 CG 6 CDG 7	HG 6 DI 3 CHG 8 CDGI 9	GI 6 DG 5 CGI 8 CDF 5	HGI 8 DGI 7 CHGI 10	F 2 DF 3 CF 4	HF 4 DFI 5 CHF 6
480 V Pump Motor-starter	Fail to start	D 2	DF 6	CF 6	CD 4	CDF 8	F 4		
	Trips pump	H 2 CD 4	F 4 CDF 8	HF 6	D 2	DF 6	CH 4	CF 6	CHF 8
Manual Valve 2" or greater	Closes	H 2	HI 4(a)	D 1	DI 3(a)	CH 4(a)	CHI 6(a)	CD 3(a)	CDI 5(a)
Check Valve 2" or greater	Fails to open	H 2 CD 3(a)	G 2 CDG 5(a)	HG 4(a)	D 1	DG 3(a)	CH 4(a)	CG 4(a)	CHG 6(a)
SIS Relays	Fail to energize	CDI 2							
CLS Relays	Fail to energize	CF 3							
Pressure Transducers	Fail to low pressure	CDI 2							
	Fail to show high pressure	CF 3							
Power Supplies	Hi voltage	CDI 2							
	Low voltage	CF 3							
Signal Comparators	Drift down	CDI 2							
	Drift up	CF 3							
Level Transmitters	Fail to show low level	CDI 2							
Bellows Joints	Rupture	G 2							

(a) Valves used in C, F, G, and I systems have manufacturers different from those used in D and H systems.

(b) For small LOCA where D includes the HPIS.

TABLE IV 5-2 INTERFACE EXAMINATION RESULTS

Affected Sequence	Interface	Discussion
HF	Containment Sump	
F	Containment Environment	Both inside CSRS pumps could be failed by post-LOCA environment. But, 2 outside CSRS pumps would remain.
CD	None	Interfaces are ruled out since they fail systems assumed to succeed.
CDI	RWST	
D	SICS	
CI	Operator	Valve positioning failures after a CSIS flow test.
CF(G,I)	CLCS	
G HG(given S)	Intake canal	Draining the intake canal fails the service water supply for the CHRS. This failure also fails the HPRS, which is not required for a large LOCA.

TABLE IV 5-3 ELECTRICAL POWER INTERFACES

		Systems Affected										
Bus Identifiers		C CSIS	F CSRS	I NaOH	D LPI	H LPR	D[(b)] HPI	H[(b)] HPR	G CSHX	SICS	CLCS Hi	CLCS Hi-Hi
JA00	4160-1J						X	X				
JB00	4160-1H						X	X				
JC00	480-1J	X	X		X	X			X			
JD00	480-1H	X	X		X	X			X			
JE00	1J1-1						X	X	X[(a)]			
JF00	1H1-1						X	X	X[(a)]			
JG00	1J1-2	X		X	X	X	X	X				
JH00	1H1-2	X		X	X	X	X	X				
JJ00	DC-1B	X	X		X	X	X	X	X	X	X	X
JK00	DC-1A	X	X		X	X	X	X	X	X	X	X
	VB1-I						X	X			X	X
	VB1-II										X	X
	VB1-III						X	X			X	X
	VB1-IV						X	X			X	X

(a) With loss of station power

(b) For small LOCA

TABLE IV 6-1 SEQUENCE AE-LLOCA/ECI, PRINCIPAL COMMON MODE POSSIBILITIES AND EFFECTS

Common Mode Failure	Effect
1. LLOCA in one CSIS injection line.	1. Failure probability of ECI increases however, failure probability of LLOCA decreases because of specific location, with net effects leading to cancellation.
2. Similar power relays fail on safety buses.	2. Already covered on fault tree and not dominant failure.
3. Pipe or valve rupture on one CSIS subsystem causes rupture of pipe or valve on adjacent selected LPCIS line or vice versa.	3. Probability of ruptures is small compared to other contributors, and commom mode combination would have no impacting contribution to ECI failure probability.
4. Damage to sensing switches in racks 25-5 and 25-6 caused by secondary failure (fire, explosion, pipe burst) preventing the generation of initiating signals to CSIS and LPCIS valves and motors.	4. Probability of secondary environment at the time of, and independent of, the LOCA is more remote than the failure probability for ECI. The overall probability is further reduced by structural protection such as the barrier between racks 25-5 and 25-6.
5. Damage to relays located on the 9-32 and 9-33 panels in the cable spreading room caused by secondary failures (fire, explosion, pipe burst) preventing the generation of initiation signals to CSIS and LPCIS valves and motors.	5. Not impacting due to same reasons indicated in 4.

TABLE IV 6-2 SEQUENCE AI-LLOCA/LPCRS, PRINCIPAL COMMON MODE POSSIBILITIES AND EFFECTS

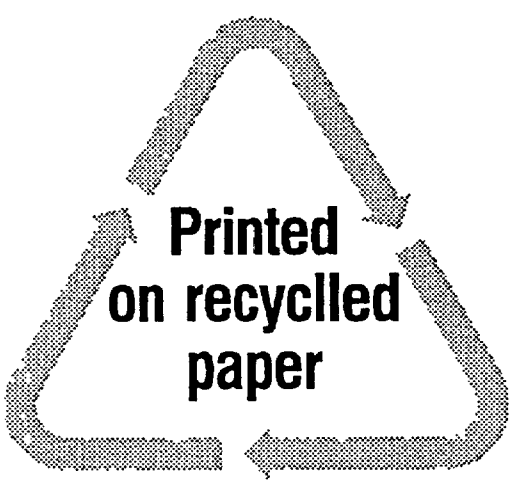
Common Mode Failure	Effect
1. Loss of emergency service water to all four pump room coolers.	1. This already is included as the dominant contribution to LPCRS failure.
2. Damage to both LPCIS injection lines in drywell by LOCA.	2. Only plugging of both lines would be significant since break in drywell would permit flow to torus while CSCRS provided the continuous core flooding. Physical arrangement of LPCIS lines makes plugging of both caused by LOCA an extremely remote possibility.
3. Failure of both LPCIS injection valves to open due to common component fault.	3. This effect can be negated by switching flow to torus through the test lines, bypassing the problem.
4. Failure of LPCIS contribution to ECI success (success mode which requires all CSIS contribution, no LPCIS).	4. Those failures which could cause loss of all LPCIS (instead of 2/4 pumps) where considered when LPCRS was evaluated.
5. Failure of all 4 LPCIS pumps or failure of 4 valves of the same type or failure of all four heat exchangers because of similar component common mode.	5. Not impacting because of the low probability of all four components of a type failing in the same time frame.
6. Rupture of ESW supply in torus compartment by LOCA in HPCI or RCIC steam supply line and resultant failure of LPCIS pumps by loss of room coolers.	6. Close proximity of HPCI or RCIC supply and ESW lines has been compensated for to some extent by restraints in the supply lines. Also, RCS rupture in these supply lines can be isolated and the core water loss stopped. The resultant special sequence of required failures does not dominate the consequence probability results.

TABLE IV 6-3 SEQUENCE AJ-LLOCA/HPSW, PRINCIPAL COMMON MODE POSSIBILITIES AND EFFECTS

Common Mode Failure	Effect
1. Rupture of HPSW line in torus compartment by LOCA in HPCI or RCIC steam supply line.	1. A HPSW line passes within about 6 feet of the HPCI supply line in the torus compartment. The HPCI line is restrained at expected break points and the surmised HPSW line break does not itself cause loss of HPSW. It reduces the available pumps from 4 to 2 and requires continued closure of the normally closed HPSW cross over valve at the pump building. The net effect of this common mode failure is assessed to not influence the release probability.
2. Failure of all 4 HPSW pumps or failure of 4 valves of the same type or failure of HPSW side of all four heat exchangers because of similar component common mode.	2. Not significant because of the relatively lower probability of all four components of a type failing in the same time frame.

TABLE IV 6-4 SEQUENCE S_1E-SMALL LOCA (1)/ECI, PRINCIPAL COMMON MODE POSSIBILITIES AND EFFECTS

Common Mode Failure	Effect
1. HPCIS supply line is the LOCA site inside drywell between steam header and first isolation valve.	1. HPCIS is lost raising failure probability. Failure probability decreases however because of specific location. Net effect is judged to be within error spread of failure sequence.
2. HPCIS supply line is the LOCA site inside drywell between steam header and first isolation valve and effects of LOCA fail ADS operate air supply lines or electrical signal lines to valve air operators.	2. Same as 1, plus ADS would fail. Chance of common mode effects is relatively small because a severed HPCI pipe which might move around would be a large LOCA and ADS would not be needed. Effects of small LOCA would be small missiles and jet forces only.
3. SLOCA in one CSIS injection line.	3. Same as large LOCA, effects tending to cancel.


Printed
on recycled
paper